MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN - CASO DE ESTUDIO EN LA DEPENDENCIA DE ADMISIONES, REGISTRO Y CONTROL ACADÉMICO DE LA UNIVERSIDAD DEL MAGDALENA

IVONNE PATRICIA CABARCAS HERRERA

ELSY AZENETH CANTILLO CABARCAS

VANESA JUDITH VILORIA MACHADO

UNIVERSIDAD DEL MAGDALENA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SANTA MARTA, D.T.C.H.

2008

MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN - CASO DE ESTUDIO EN LA DEPENDENCIA DE ADMISIONES, REGISTRO Y CONTROL ACADÉMICO DE LA UNIVERSIDAD DEL MAGDALENA -

IVONNE PATRICIA CABARCAS HERRERA

ELSY AZENETH CANTILLO CABARCAS

VANESA JUDITH VILORIA MACHADO

Proyecto de grado para optar al título de Ingeniero de Sistemas

Directora:

MAYDA PATRICIA GONZÁLEZ ZABALA

Magíster en Informática

Codirector:

LUIS CARLOS GOMEZ FLOREZ, MSc.

UNIVERSIDAD DEL MAGDALENA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SANTA MARTA, D.T.C.H.
2008

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del jurado

_____
Firma del jurado

Santa Marta, julio 28 de 2008

DEDICATORIA

A Dios, por darme sabiduría en esta fase de mi vida.

A mi madre, por su apoyo, confianza y sobre todo por ayudarme a ser una profesional.

A Deti, por su apoyo en los momentos difíciles.

A Enrique, por su apoyo incondicional y su amor de padre.

A Víctor y a Elías, por ser tan especiales y llenar mi corazón de ternura.

A Alexander por su apoyo incondicional en todo tiempo, por su paciencia, su cariño y amor.

A mis dos grandes amigas, que me soportaron todo el tiempo, y fueron de gran apoyo en esta ciudad.

IVONNE

Dedicado a:

Dios por haber sido la luz que me ha guiado
para conseguir este gran logro.

Mis padres DAGOBERTO y BILDA por tenerme paciencia,
dedicación y brindarme apoyo en todo momento.

Mis hermanos ELIANA, DARLY e IVAN,
por apoyarme siempre.

Mis sobrinos SALENI, MAILYN y AIMAR por llenar
mi vida de alegría y gratos momentos.

Mis amigas y a todas aquellas personas que de alguna u
otra forma me brindaron su apoyo en las dificultades
y celebran conmigo mis triunfos.

ELSY

Dedicado:

A Dios
Por darme vida para cumplir uno de mis sueños,
fortaleza en el momento que más lo necesite y
sabiduría en el desarrollo de la investigación.

A mi mami y a papá
Por su gran apoyo, esfuerzo, confianza e infinito amor,
por ensañarme que se debe luchar por lo que se quiere
Y por que sin ellos no hubiese sido posible.

A quien me ayudó a construir y a cumplir mis sueños.

A mi familia y a mis amigas
que fueron mi compañía en este camino

VANESA

AGRADECIMIENTOS

Al Ingeniero. MSc Luís Carlos Gómez Flórez, Codirector del proyecto de investigación, por sus enseñanzas y valiosa colaboración en la fase inicial del proyecto.

A la Ingeniera Mayda González Zabala, directora de esta investigación, por su orientación y sus importantes aportes en el desarrollo de esta investigación.

Al ingeniero Samuel Prieto Mejía, director de la dependencia de Admisiones Registro y Control Académico de la Universidad del Magdalena, por su colaboración en la aplicación de esta investigación.

Al personal que labora en la dependencia de Admisiones Registro y Control Académico de la Universidad del Magdalena, por su colaboración y disponibilidad en la aplicación de esta investigación.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

GLOSARIO JURÍDICO TECNOLÓGICO

Acción de tutela: es la garantía constitucional del derecho que tiene toda persona a la protección judicial de sus derechos fundamentales a través de un recurso efectivo.

Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de diversos recursos.

Bases de datos: es un conjunto de datos organizados en una estructura que facilite su almacenamiento y recuperación, diseñada para facilitar su mantenimiento y acceso de una forma estándar.

Campo: se refiere a un tipo o atributo de información.

Corte Constitucional: es un organismo perteneciente a la rama judicial del Poder Público y se le confía la guarda de la integridad y supremacía de la Carta Política. Fue creada por la actual Constitución Política, vigente desde el 7 de julio de 1991. Algunas de sus funciones consisten en decidir sobre las demandas de constitucionalidad que promuevan los ciudadanos contra las leyes; decidir sobre la constitucionalidad de los referendos sobre leyes, las consultas populares y los plebiscitos del orden nacional; ejercer el control constitucional sobre los decretos legislativos dictados por el Gobierno al amparo de los estados de excepción; decidir definitivamente acerca de las objeciones por inconstitucionalidad que el Gobierno formule contra proyectos de ley y de manera integral y previa respecto a los proyectos de ley estatutaria aprobados por el Congreso.

Dato: es el valor que toma o identifica un atributo o variable en un caso particular.

Datos personales: Se trata de la información de cualquier tipo referida a las personas físicas o de existencia ideal determinadas o determinables.

Datos sensibles: aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Derechos: conjunto de normas que constituyen el ordenamiento jurídico vigente de un país.

Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos o recursos.

Indicador: es la valoración de una o más variables que informa sobre una situación y soporta la toma de decisiones, es un criterio de medición y de evaluación cuantitativa o cualitativa.

Informática jurídica: es la aplicación de la Técnica Informática a la ciencia del Derecho; es decir, cuando se asumen las tecnologías de información como una herramienta del operador jurídico

Legislación: Conjunto o cuerpo de leyes por las cuales se gobierna un Estado, o una materia determinada.

Ley estatutaria: regula los derechos y deberes fundamentales de las personas y los procedimientos y recursos para su protección; la organización y régimen de los partidos y movimientos políticos; el estatuto de la oposición y funciones electorales; las instituciones y mecanismos de participación ciudadana; los

Estados de excepción y un sistema que garantice la igualdad electoral entre los candidatos a la Presidencia de la República". El constituyente optó por regular su trámite con especificidades y requisitos adicionales a los de cualquier ley ordinaria.

Ley ordinaria: regulan la gran mayoría de temas respecto de los cuales se puede legislar, son genéricas y el constituyente no consideró oportuno establecer requisitos de procedimiento especiales o mayorías cualificadas para su aprobación.

Medidas técnicas: permiten conservar la integridad de la información y la confidencialidad de los datos personales, estas se aplican sobre los sistemas de información, bases de datos, equipos y lugares donde estos se ubican, al igual que en todos los elementos materiales que tratan los datos.

Medidas Organizativas: procuran garantizar la confidencialidad, integridad y seguridad de los datos almacenados en programas y sistemas de información de una organización, estas medidas establecen los procedimientos, normas, reglas y estándares de seguridad, en los usuarios o personal que manejan los datos almacenados en las bases de datos.

Normativa: Conjunto de normas aplicables a una determinada materia o actividad.

Registro: se refiere a toda la información sobre un individuo.

Reglamentación: conjunto de órdenes y reglas que rigen a un país.

Restauración de datos: hace referencia a las técnicas empleadas para recuperar archivos que han sido perdidos o eliminados de algún medio de almacenamiento.

Seguridad informática: consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean

utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Soporte informático: objeto físico (diskette, CD, disco duro, memoria USB) susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

Tecnología de Información (TI): trata sobre la utilización de tecnología, específicamente computadoras y ordenadores electrónicos, para el manejo y procesamiento de información, como la captura, transformación, almacenamiento, protección, y recuperación de datos e información.

Titular de la información: Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

Tratamiento de datos personales: esta expresión se entiende como cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recolección, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

INTRODUCCIÓN

En la actualidad, el vertiginoso avance en las tecnologías de la información, su inclusión en la vida diaria de las personas y en las organizaciones de carácter público y privado, su constante utilización y la acumulación de grandes cantidades de información personal, ha cambiado los procesos y costumbres de nuestra sociedad; generando nuevas formas de delitos, abusos y crímenes que amenazan valores sociales y la privacidad individual, de igual forma esto ha generado la creación de nuevas leyes y conceptos jurídicos que buscan la protección de las personas en relación con el tratamiento que se le da a su información, por tal razón ha surgido el derecho de protección de datos personales que hace parte del derecho informático, que se encarga de regular los actos y hechos delictivos o poco éticos derivados de la informática.

Sin embargo, la existencia de leyes en este ámbito, no son suficiente garantía para que las personas se sientan seguras en la forma como es manipulada o utilizada su información personal por parte de los operadores de información en las organizaciones, puesto que algunas veces las leyes resultan poco eficaces para interpretar la realidad, ya que se puede encontrar dificultad para adaptar las leyes a los cambios tecnológicos que se están presentando, por tal motivo se hace necesario diseñar mecanismos o herramientas tecnológicas que evalúen, garanticen y permitan adaptar los sistemas de información a las leyes establecidas, ya que estas por sí sola no son suficientes para proteger dichos datos y proteger los derechos de las personas por el uso y administración inadecuada de la información; teniendo en cuenta que al no proteger debidamente la información almacenada en bases de datos puede causar perjuicio al titular de dichos datos.

Lo anterior, fue motivo para plantear y desarrollar la propuesta de investigación titulada “Modelo para estudiar y evaluar el cumplimiento de los derechos de protección de datos en los sistemas de información -Caso de Estudio la Dependencia de Admisiones, Registro y Control Académico de la Universidad del Magdalena-”, el cual se constituye en un mecanismo para estudiar y evaluar en que medida se cumplen los derechos de protección de datos en los sistemas de información, así mismo permite que al implementar las recomendaciones dadas en la evaluación se pueda garantizar dichos derechos y se pueda evitar la violación de estos, con lo cual se aporta a las organizaciones en mejorar el buen uso y administración de la información en sus sistemas de información

El presente documento expone el desarrollo de la investigación realizada, iniciando con la presentación de la propuesta investigativa, seguido del marco de ideas que sustenta el desarrollo de este estudio, las diferentes actividades realizadas en todo el proceso de investigación y los resultados obtenidos, el cual consiste en el desarrollo del modelo planteado y la experiencia obtenida en el caso de estudio aplicado en el desarrollo de la investigación.

1 GENERALIDADES DE LA PROPUESTA DE INVESTIGACIÓN

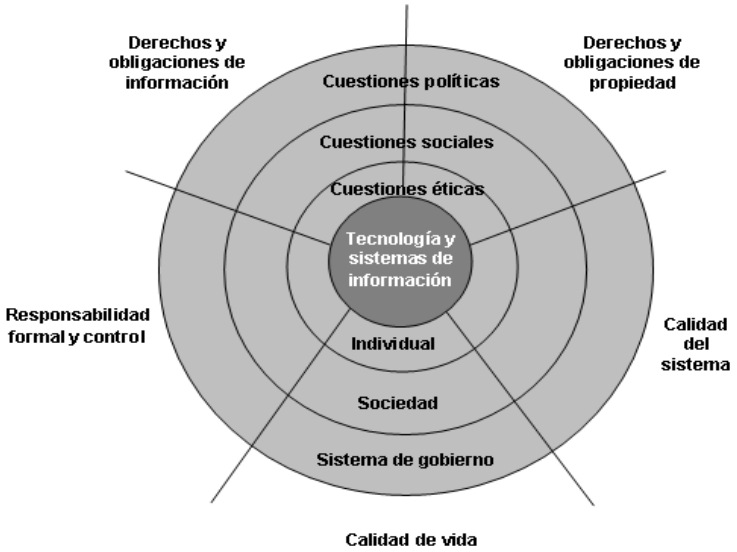
Este capítulo presenta la propuesta que origina la realización del proyecto, en este se encuentra inicialmente la relación entre la tecnología de información con los aspectos éticos, sociales y políticos, para explicar seguidamente la situación problema de la investigación, la importancia de esta, los objetivos formulados, la metodología a utilizar, y posteriormente se describe la manera como están organizados los capítulos en este proyecto.

1.1 TECNOLOGÍA DE INFORMACIÓN Y SU RELACIÓN CON ASPECTOS ÉTICOS, SOCIALES Y POLÍTICOS

Según Laudon y Laudon [1], la tecnología de información ha evolucionado tanto en los últimos años, que se ha convertido en un mecanismo potente para el crecimiento de la economía y la transformación de la sociedad, pero así como esta puede servir para lograr un progreso social, también pueden servir para cometer crímenes y amenazar valores sociales, convirtiendo esto en un problema ético. Este problema se ha incrementado debido a cuatro tendencias tecnológicas, las cuales son: *la duplicación de la capacidad de cómputo*, ya que la mayoría de las organizaciones que utilizan sistemas de información en sus procesos, han aumentado su dependencia hacia estos, generando vulnerabilidad ante los errores de los sistemas y los datos de mala calidad. Otras tendencias tecnológicas son *los adelantos en las técnicas de almacenamiento, la extracción de datos* y *el trabajo con redes* (incluyendo Internet), que han reducido el costo, aumentando la facilidad de comunicar, copiar y manipular información, aún en los entornos en línea, lo cual hacen que se desafíen las reglas tradicionales (ética) en cuanto a una conducta correcta e incorrecta; todo lo anterior ha creado nuevas oportunidades para el abuso y delito en los sistemas de información, violando así la privacidad individual.

De este modo, las personas enfrentan cuestiones éticas cuando deben decidir como proceder en una situación en la que sus principios éticos están en conflicto (dilema). Asimismo, los aspectos sociales provienen de las cuestiones éticas, por eso la sociedad debe crear en los individuos expectativas acerca de una conducta correcta, en consecuencia los aspectos sociales producen controversias entre los tipos de situaciones y las expectativas que la sociedad debe difundir para que los individuos se comporten de una manera correcta. Estas cuestiones sociales se reflejan en los aspectos políticos, los cuales tienen que ver con las leyes que establecen la conducta y tratan de crear situaciones en las que los individuos se comportan correctamente. Sin embargo, las cuestiones éticas, sociales y políticas se relacionan con cinco dimensiones morales, las cuales son: derechos y obligaciones de información, derechos de propiedad, responsabilidad formal y control, calidad del sistema y calidad de vida. Finalmente, la relación entre aspectos éticos, sociales y políticos en una sociedad de información se ilustra en la figura 1.

Figura 1. Relación entre aspectos éticos, sociales y políticos en una sociedad de información**.**



Fuente: LAUDON C, Kenneth y LAUDON P, Jane. 2002. P.128

Ante esta necesidad surge una nueva responsabilidad legal[1] con la sociedad, el habeas data y la protección de datos personales, el cual lleva consigo un compromiso de parte de las organizaciones en hacer cumplir estos derechos en sus sistemas de información, implicando una responsabilidad formal, que establece mecanismos para evaluar la responsabilidad de las decisiones tomadas y las acciones realizadas, tal como es el caso del estándar Cobit*–(Control Objectives for Information and Related Technology- Objetivos de Control para la Información y Tecnologías Relacionadas), que especifica unos criterios de control llamados requerimientos de información del negocio, los cuales distinguen siete categorías que son las bases de su trabajo, y uno de ellos es el requerimiento de cumplimiento, el cual tiene que ver con acatar leyes, reglamentos y acuerdos contractuales que está sujeto al proceso de negocio[2].

1.2 PLANTEAMIENTO DE LA SITUACIÓN DE INTERÉS

En la sociedad de la información se recurre cada vez más al tratamiento de datos y a las tecnologías, las cuales facilitan considerablemente la captura, transferencia, registro y conservación de estos; sin embargo con la ayuda de herramientas claves como lo es el Internet, se puede dar un indebido uso de la información, por lo tanto se hace necesario proteger de manera especial los datos personales[3] de cada individuo.

---

1 La responsabilidad legal es una característica de los temas políticos en los que hay leyes que permiten a los individuos ser compensados por los perjuicios infligidos en ellos por otros autores, sistemas u organizaciones.

* COBIT es un marco de referencia y un juego de herramientas innovadora para el gobierno de tecnologías de información que ayuda a la gerencia a comprender y administrar los riesgos asociados con la tecnología de información.

2 Para mayor información consultar www.isaca.org/cobit

3 Según Nelson Remolina Angarita, los datos personales hacen referencia a cualquier aspecto de la persona, como se muestra a continuación.

(i) datos biográficos (nombre, fecha y lugar de nacimiento, domicilio, nacionalidad, raza y sexo, entre otros).
(ii) datos sobre el domicilio (dirección, teléfono, barrio, estrato socio económico, entre otros).
(iii) datos familiares (estado civil; nombre de padres y hermanos, número y nombre de hijos, entre otros).
(iv) datos laborales (nombre del empleador, nombre del jefe, cargo, salario, responsabilidades, dirección, fax, teléfono, dirección electrónica, horario de trabajo, entre otros).
(v) información financiera (ingresos, seguros, saldo promedio, número de cuentas de ahorro o corriente; número de tarjetas de crédito, comportamiento financiero, entre otros).
(vi) información médica (grupo sanguíneo, enfermedades, alcoholismo, uso de medicamentos, entre otros).
(vii) información ideológica (pertenencia a partidos políticos y sindicatos, comportamiento respecto la frecuencia a votar, religión, entre otros).

Una evidencia de lo anteriormente mencionado son las encuestas realizadas en Europa[4], las cuales demuestran la preocupación de los ciudadanos en cuanto al manejo que las organizaciones le dan a sus datos personales; aproximadamente el 64% de los encuestados expresaron estar preocupados sobre la protección de su información personal, el 82% de los encuestados señaló que la transmisión de datos a través del Internet no es lo suficientemente segura, solamente el 22% de los usuarios utilizan herramientas y tecnologías (firewalls y cookies) que aumentan la seguridad de los datos a través de la red.

Otra evidencia, según Remolina [2], es la existencia de compañías como ChoicePoint Online que ofrecen a cualquier persona el servicio de acceder rápidamente por Internet información confidencial, como datos de identificación, incluyendo fecha y lugar de nacimiento, número de pasaporte, número de identificación nacional, descripción familiar y física, entre otras cosas; por esta información de ciudadanos de diferentes países de Latinoamérica, la compañía en el año 2002 recibió millones de dólares.

Asimismo, en Colombia se ha presentado casos del uso indebido de datos personales que han causado perjuicio a las personas a quien se refiere dicha información. Según Remolina [3], algunos de estos casos son los siguientes:

(viii) información académica (colegios y universidades, títulos obtenidos, calificaciones, investigaciones disciplinarias, entre otros).
(ix) Información policíaca (infracciones, licencia de conducir, detenciones preventivas, entre otros).
(x) Pasatiempos (actividades deportivas, tipos de lectura preferida, programas de televisión, hobbies, lugares visitados en vacaciones, entre otros).
(xi) Hábitos (lugares normalmente frecuentados, clase de libros adquiridos, tipo de ropa utilizada, entre otros).
(xii) Información sobre viajes y comunicaciones (uso de transporte público, aerolínea o empresa de transporte frecuentemente utilizada, celular, bipper, sitios preferidos para pasar las vacaciones).
(xiii) Información patrimonial (bienes inmuebles y muebles, obligaciones pecuniarias, ubicación de bienes, actividad económica que desarrolla, entre otros)

[4] Publicada por el Directorado General de Justicia, Libertad y Seguridad de la Comisión Europea en febrero del 2008.

- La utilización de datos personales para exterminar personas por su origen racial o étnico o para “reubicarlos” y desplazarlos en campos de concentración.
- Personas capturadas indebidamente por información desactualizada e incorrecta en las bases de datos de organismos del Estado.
- La utilización de datos por grupos ilegales para chantajear y secuestrar.
- El registro de información errónea en los sistemas de información.

Un ejemplo de los casos anteriores, es lo sucedido con alias "Simón Trinidad", quien, según la prensa, cuando ingresó a las filas de la guerrilla se llevó consigo información sobre los clientes del Banco del Comercio de Valledupar. Estos datos personales de los clientes se utilizaron posteriormente para decidir qué personas serían objeto de extorsiones y secuestros con fines económicos.

Por todas estas razones, emerge una necesidad de proteger los derechos que las personas tienen a actualizar, rectificar o borrar sus datos de cualquier sistema de información, creando mecanismos que sirvan de apoyo para evaluar el cumplimiento de las leyes que protegen datos personales. La propuesta surge como alternativa de solución, la cual se fundamenta en construir un modelo que al ser aplicado en los procesos de una organización que utilizan datos personales y son apoyados por sistemas de información, permita estudiar y evaluar el cumplimiento de los derechos de protección de datos en los sistemas de información, para garantizar el derecho del habeas data al titular de los datos. El modelo proporciona una guía que define los mecanismos de recolección de información que serán utilizados en la aplicación del modelo, los cuales permitirán evaluar el cumplimiento de los derechos de protección de datos teniendo en cuenta los criterios de medición definidos, además se presenta un esquema para analizar la información recolectada, luego determina el estado del nivel de cumplimiento de estos derecho en el sistema ha evaluar, finalmente se plantean

recomendaciones tanto administrativas como técnicas al caso de estudio señalado.

1.3 JUSTIFICACIÓN

Este proyecto de investigación estudia un tema actual y de gran importancia para nuestra región y para la seguridad informática; esta propuesta pretende desarrollar una metodología que permita evaluar el cumplimiento de los derechos de protección de datos, convirtiéndose esta en una de las primeras investigaciones que realiza la Universidad y la región en materia de protección de datos; de igual manera, este proyecto se puede tomar como base para la construcción de herramientas software que sirvan de apoyo tecnológico y faciliten la realización de auditorías en sistemas de información.

Aunque en la actualidad la legislación existente relacionada con la Informática sigue siendo escasa, en los últimos años los gobiernos empiezan a tomar conciencia de la necesidad de exigir responsabilidades en los riesgos derivados de los sistemas informáticos y de establecer controles adecuados. Este proyecto pretende suministrar una herramienta que permita la realización de una auditoria de protección de datos de acuerdo al nivel de las leyes definidas para el país.

Por otra parte, el desarrollo de este proyecto de investigación tiene como base las doctrinas del derecho, principios y leyes de protección de datos a nivel nacional e internacional, aplicando conocimientos de informática, al igual que conocimientos adquiridos a lo largo del desarrollo de la investigación con respecto al tema de protección de datos y administración de la información, y otros temas relacionados con la ingeniería de sistemas y el derecho informático; además se pretendió realizar un aporte al campo de la informática jurídica, creando mecanismos para apoyar el cumplimiento de estas leyes y mejorar de forma significativa la administración de los datos personales en los procesos asistidos por sistemas de información que utilizan este tipo de datos.

Por lo tanto las organizaciones que apliquen el modelo propuesto, pero sobre todo que lleven a cabo las recomendaciones planteadas en la última etapa del modelo, garantizarán una mejor administración de los datos personales, los cuales serán en lo posible completos, exactos, actualizados, comprobables, comprensibles, que cumplan con una finalidad establecida, que tengan un tratamiento especial a datos referidos al origen racial y étnico, ideología, afiliación sindical, religión, opiniones políticas, creencias, salud, o vida sexual; que tengan medidas técnicas que garanticen su seguridad; que su transferencia sea confiable; de tal manera que todo lo anterior garantice la protección de datos personales, evitando sanciones por mal uso de esta información.

1.4 OBJETIVOS

1.4.1 Objetivo general

Definir un modelo que permita estudiar el cumplimiento de los derechos de protección de datos, evaluando los Sistemas de Información, para garantizar el derecho del habeas data, ilustrando como caso de estudio, su aplicación en la dependencia de Admisiones, Registro y Control Académico de la Universidad del Magdalena.

1.4.2 Objetivos específicos

- Analizar las doctrinas del derecho y las leyes que rigen el cumplimiento de la protección de datos en los sistemas de información, a nivel nacional e internacional.

Se realiza un estudio de las leyes de protección de datos a nivel nacional e internacional para definir los derechos de protección de datos que evaluará el modelo.

- Construir un modelo basado en el estudio realizado que contenga las siguientes funciones:

  - Definir los mecanismos de recolección de información, tales como: encuestas, formularios, cuestionario de entrevistas, observaciones directas del sistema, etc.

  - Analizar la información recopilada por el modelo, teniendo en cuenta las leyes de la protección de datos y los indicadores de evaluación, para verificar el cumplimiento de estos en un sistema de información.

  - Presentar los resultados obtenidos de la aplicación mediante los indicadores de evaluación.

Se crea un modelo a partir del estudio de las leyes de protección de datos, el cual propone y define los mecanismos de recolección de información ideales para la aplicación del proyecto; evalúa el cumplimiento de los derechos de protección de datos a través de los criterios de evaluación, y analiza los resultados obtenidos; además el modelo indica el nivel de cumplimiento en que se encuentra el sistema de información.

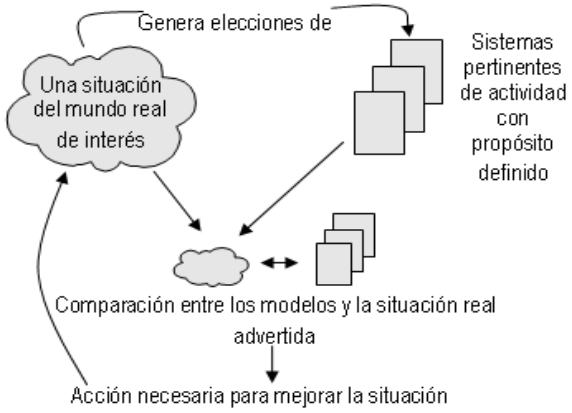
- Ilustrar la aplicación del modelo propuesto al caso de estudio de la dependencia de Admisiones, Registro y Control Académico de la Universidad del Magdalena.

Una vez construido el modelo se procede a utilizarlo en un caso de estudio, la dependencia de Admisiones, Registro y Control Académico de la Universidad del Magdalena, el cual evaluará el cumplimiento de los derechos de protección de datos y formulará recomendaciones a su sistema de información.

1.5 METODOLOGÍA PROPUESTA

Para la realización de este proyecto se utilizará la Metodología de los Sistemas Blandos (MSB), propuesta por Peter Checkland, la cual está basada en el pensamiento de sistemas y es aplicable para la toma de acción con propósito definido que intente cambiar situaciones reales de una manera constructiva; es decir, que esta metodología tiene como objetivo mejorar la situación que se considera problemática dentro de una organización, para ello se tienen en cuenta diferentes puntos de vista relacionados a ¿qué hay que hacer? y ¿cómo hacerlo?, los cuales podrían mejorar esa situación, generando un debate que finaliza con la implementación de cambios deseables y viables para la organización. La forma básica de la MSB se ilustra en la Figura 2.

Figura 2. Forma básica de la metodología de sistemas blandos



Fuente: CHECKLAND, Peter y SCHOLES, Jim. 1994. P.23

1.6 DESCRIPCIÓN DE LA ESTRUCTURA DEL DOCUMENTO

La presente investigación tiene 6 capítulos, los cuales describen las etapas desarrolladas en su elaboración, a continuación se presenta la forma en que se encuentra organizado el presente documento:

Se inicia con el *capítulo 1*, *Generalidades de la Propuesta de Investigación*; el cual tiene como fin ubicar al lector en el contexto en el cual se desarrolló el proyecto y

la situación problema que dio origen a la realización de este estudio, seguida de la descripción de la propuesta de investigación y la presentación de los objetivos.

El *capítulo 2, Marco Teórico y Metodológico del Proyecto de Investigación*; describe los fundamentos teóricos y metodológicos bases para el desarrollo de la investigación, los cuales ayudan a tener una conceptualización de lo que se va a realizar, la manera como se llevará a cabo la propuesta de investigación, la relación existente entre informática y el derecho, el habeas data y la protección de datos y los mecanismos para la recolección de información.

El *capítulo 3*, *Análisis de las Leyes de Protección de Datos a Nivel Internacional y Nacional;* estudia las doctrinas del derecho y las leyes que rigen el cumplimiento de la protección de datos en los sistemas de información, a nivel nacional e internacional; el cual presenta los fundamentos conceptuales para los derechos de protección de datos, un resumen de los países que poseen leyes de protección de datos en Europa y América, luego se elabora una comparación entre estas leyes para definir los derechos de protección de datos que se evaluarán en los sistemas de información.

El *capítulo 4*, *Diseño del Modelo para Evaluar el Cumplimiento de los Derechos de Protección de Datos en los Sistemas de Información*; presenta el Sistema de Actividad Humana – SAH propuesto para desarrollar la propuesta de investigación, guiados por la metodología de Sistemas Blandos – MSB, planteada por Peter Checkland. En este diseño se tiene en cuenta los derechos de protección de datos establecidos en el capítulo anterior, los factores que influyen en la evaluación de estos derechos y los indicadores de evaluación que permiten analizar la información recopilada y verificar el cumplimiento de estos derechos en un sistema de información.

El *capítulo 5*, *Aplicación del Modelo al Caso de Estudio*, ilustra la aplicación del modelo propuesto al caso de estudio seleccionado, presentando los resultados obtenidos mediante los indicadores de evaluación. Finalmente se dan las recomendaciones para cumplir con los principios de protección de datos y las conclusiones de la aplicación del modelo.

El *capítulo 6*, *Conclusión*; expone las conclusiones generales obtenidas del desarrollo del proyecto de investigación.

2 MARCO TEÓRICO Y METODOLÓGICO DEL PROYECTO DE INVESTIGACIÓN

En este capítulo se presentan los fundamentos teóricos y metodológicos que sustentan el desarrollo de esta investigación, los cuales han sido tomados y adaptados de diferentes fuentes de investigación y pertenecen a autores especializados en cada tema.

2.1 MARCO TEÓRICO

En esta sección se muestran los conceptos utilizados a lo largo del desarrollo de la investigación, tales como modelos, sistemas de información, auditoría informática, derecho informático, así mismo se presentan las áreas de estudio de este último, entre estas la Protección de Datos, tema principal de estudio en este proyecto de investigación y finalmente se explica lo referente al Habeas Data, destacando su definición, importancia y clasificación.

2.1.1 Definición general de modelo

Tomando el concepto de modelo de Burch [4] se cita la siguiente definición:

> *"Los modelos son una forma de abstracción o representación de la realidad. Generalmente son una simplificación de una cosa real. En los sistemas de información, el analista de sistemas debe construir diversos modelos con varios propósitos. Uno de los propósitos puede incluir el desarrollo de un conjunto de procedimientos que debe seguir el personal para llevar acabo ciertas tareas".*

En términos generales, se puede decir que un modelo es la interpretación que cada individuo da de una realidad observada desde su punto de vista; y que este puede servir como mecanismo para realizar un análisis de la simplificación de un proceso o una situación de interés y compararlo con la realidad o una

aproximación de esta, teniendo en cuenta que cada persona percibe una situación de diferentes formas.

Es importante tener en cuenta las utilidades de los modelos, como por ejemplo la posibilidad que tienen los modelos de ilustrar un concepto, la estructura de un sistema, explicar las características de un sistema; pero además de ilustrar y explicar, también permiten predecir situaciones futuras, ya que pueden representar el comportamiento de un aspecto del mundo real, dando así la posibilidad de adelantarse al presente. De igual manera los modelos se utilizan como prerrequisitos para el diseño de nuevas tecnologías.

Después de definir y mostrar la importancia que tiene los modelos, se procede a describir las clases de modelos y su propósito, tomando como referencia a Russell Ackoff (1962)[5], aunque esta clasificación proporciona una distinción útil, solo cubre los modelos de forma física o que pueden controlarse de manera cuantitativa. Se distinguen tres formas de modelos los cuales son:

- ***Modelos Icónicos:*** son aquellos que se muestran en una versión en miniatura (aunque algunas veces es una ampliación) del sistema real y las propiedades relevantes de dicho sistema se representan por medio de las propiedades mismas pero, por lo general, con un cambio de escala.

- ***Modelos Analógicos:*** son los modelos que explican una realidad a través de otras situaciones que se asemejan en cuanto a su comportamiento y relaciones.

- ***Modelos Analíticos:*** en esta clase de modelo las relaciones matemáticas lógicas pueden desarrollarse de manera que representan las leyes físicas

[5] ACKOFF, Russell. Citado por WILSON, Brian. Sistemas: conceptos, metodologías y aplicaciones. México. 1993

que rigen la conducta de la situación estudiada. Dicho desarrollo, por lo general, precederá un modelo análogo.

Según Wilson [5], a esta clasificación se le debe agregar los ***Modelos Conceptuales,*** los cuales incluyen modelos pictográficos/simbólicos, en referencia a la definición, que cubre los aspectos cualitativos de la situación; y su importancia radica en que permiten identificar, organizar y realizar razonamientos sobre los componentes y comportamiento de un sistema.

2.1.2 Definición de sistemas de información

Tomando el concepto planteado por Laudon y Laudon [1], técnicamente un sistema de información es un conjunto de componentes interrelacionados que recolectan, procesan, almacenan y distribuyen información; estos no solo utilizan datos de personas, u otros elementos relacionados con la organización, conjuntamente son un apoyo y una pieza clave para controlar la información, permitiendo tomar mejores decisiones en una organización, además, los sistemas de información también ayudan a los administradores y trabajadores a analizar problemas, visualizar aspectos complejos y crear productos nuevos.

Figura 3. Sistemas de información desde la perspectiva de los negocios.

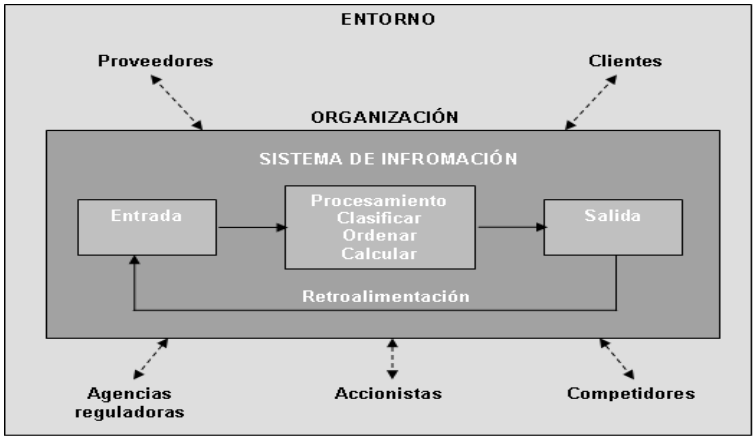
Fuente: LAUDON C, Kenneth y LAUDON P, Jane. 2002. P.10

Dando una definición desde el punto de vista de los negocios, Laudon y Laudon [1], consideran que un sistema de información es una solución organizacional y administrativa, basada en tecnología de información, a un reto que se presenta en el entorno, y que para usar eficazmente sistemas de información un administrador debe entender las dimensiones de organización, administración y tecnología de información más amplias de los sistemas (Ver figura 3) y la capacidad de éstas para solucionar los retos y problemas del entorno de negocios.

2.1.3 Etapas de procesamiento de datos en un sistema de información

Según Laudon y Laudon [6] en un sistema de información existen tres actividades que producen la información que las organizaciones necesitan para tomar decisiones, controlar operaciones, analizar problemas y crear nuevos productos o servicios. Estas actividades se muestran en la Figura 4, las cuales son entrada, procesamiento y salida. La *entrada* recolecta datos del interior de la organización como de su entorno externo. El *procesamiento* convierte, maneja y analiza los datos recolectados en información representativa para los seres humanos. La *salida* distribuye la información procesada para las personas que la utilizan en sus actividades. La *retroalimentación* es la salida devuelta a las personas o actividades adecuadas de la organización para evaluar y corregir la etapa de entrada. Además se destaca en el entorno una serie de factores como clientes, proveedores, competidores, accionistas y agencias reguladoras que interactúan con la organización y su sistema de organización.

Figura 4. Funciones de un sistema de información



Fuente: LAUDON C, Kenneth y LAUDON P, Jane. 2004. P.9.

Partiendo de la definición planteada por Laudon y Laudon [6] se analizó que en todo procesamiento de información se distinguen ciertas etapas por la que todo tratamiento automatizado de datos debe seguir, como es desde el inicio de la recolección de los datos y registro de estos al sistema, pasando por las etapas de procesamiento y almacenamiento, hasta la utilización de los datos. A continuación se presentan las etapas definidas para el procesamiento de datos:

2.1.3.1 Etapa de recolección y registro de datos

En esta etapa la organización adquiere los datos, los cuales pueden ser primarios, cuando son recolectados del mismo titular de la información, o secundarios cuando estos son recolectados por otra fuente y se proporcionan o son cedidos a la entidad. Luego de adquirir los datos, estos son registrados en el sistema de información.

2.1.3.2 Etapa de procesamiento de datos

Después que los datos son registrados, por lo general estos están sujetos a actividades de procesamiento, como cálculo, comparación, distribución, clasificación y resumen. Estas actividades organizan, analizan y manipulan los datos convirtiéndolos de esta forma en información para usuarios finales. La

calidad de cualquier dato almacenado en un sistema de información también debe mantenerse mediante un procesamiento continuo de actividades de corrección y actualización.

2.1.3.3 Etapa de almacenamiento de datos

La información procesada es almacenada en las bases de datos de los sistemas de información de la organización; en esta etapa los datos y la información se deben guardar de manera organizada y segura para su uso posterior.

2.1.3.4 Etapa de utilización de datos

Cuando los datos son procesados y almacenados, estos se convierten en información útil, la cual es necesaria para el buen funcionamiento de la organización y utilizada para la toma de decisiones; en esta última etapa se evalúa la forma en que es utilizada la información almacenada en las bases de datos de los sistemas.

Después de explicar las etapas del procesamiento de datos, en la siguiente sección se continúa con los conceptos de auditoria informática y derecho informático, los cuales se muestran a continuación.

2.1.4 Auditoría informática y derecho informático

Tomando el concepto de diversos autores tales como Echenique [7] o Piattini [8], entre otros; la auditoría informática es el proceso de recoger pruebas para determinar si un sistema informatizado protege y mantiene la integridad de los datos, cumple con los objetivos de la organización y utiliza eficazmente los recursos.

En un sistema de información se debe revisar y evaluar su utilización y eficiencia, al igual que los controles y la seguridad en el procesamiento de la información, con el propósito de lograr una utilización eficiente y segura de la información; en general, evaluar un sistema de información comprende evaluar sus entradas,

procedimientos, controles, archivos, seguridad y resultado de la información. La auditoría informática es de vital importancia para el buen desempeño de los sistemas de información, porque proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

Otro concepto a destacar, es el derecho informático definido por Téllez [9] como *"el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática".* Debido a lo anterior se puede apreciar, que el derecho de las tecnologías de la información es una relación entre el derecho y la informática, que se origina cuando se considera a la informática, en todos sus aspectos, como objeto del derecho. A continuación se muestra en la Tabla 1, las áreas de estudio del derecho de la informática.

Tabla 1. Áreas del derecho de las tecnologías de la información y las comunicaciones. Basado Davara, Miguel [17]. 2007.

Derecho de las TIC	Descripción
Protección de Datos	Se trata de las normas o leyes que reglamentan el tratamiento de datos personales, su privacidad, buen nombre y derecho a la información, ante el manejo inapropiado de informaciones que atentan contra derechos fundamentales de las personas.
Propiedad Intelectual e Industrial	Derechos que corresponden por ley al autor de una creación desde el momento en que toma una forma en cualquier tipo de soporte tangible, ya sea papel o medio magnético.
Protección Jurídica del Software	Se refiere a la legislación de protección de la propiedad intelectual al software y productos registrados en medios electrónicos.
Contratos informáticos	Convenios de contratos o pagos utilizando redes de comunicación.
Comercio electrónico (pago electrónico, nombres de dominio, ...)	Realización de actividades que tiene por objeto realizar una operación comercial, a través de medios o herramientas electrónicas.
Firma electrónica	Transferencia al entorno electrónico de la firma manuscrita en papel, sirviendo así como medio para determinar la autoría de cualquier documento electrónico que pueda ser transmitido a través de redes de comunicaciones.
Delitos y Fraudes informáticos	Se produce mediante la utilización de sistemas de información para el cometido de un delito.
Telecomunicaciones	Todo lo referente a la legislación de las actividades realizadas por

Derecho de las TIC	Descripción
	cualquier medio de transmisión de datos, en el sector de las telecomunicaciones.

Cabe anotar, que este proyecto de investigación es enfocado en el derecho informático, y el presente estudio se realizó más específicamente en los derechos de protección de datos, el cual hace parte de esta área y es el tema de interés para esta investigación.

2.1.5 Derechos de protección de datos y habeas data

Según Remolina [10], la protección de datos se define como el conjunto de normas y principios que regulan el tratamiento de datos personales en todas las etapas (recolección, almacenamiento, circulación, publicación y transferencia nacional e internacional). Dicho de otra forma, la protección de datos personales es la protección jurídica de las personas en el tratamiento de sus datos de carácter personal, y es la defensa de los ciudadanos contra la posible utilización de sus datos por parte de terceros, en forma no autorizada, que puedan afectar su entorno personal, social o profesional.

Conociendo que la protección de datos se origina como respuesta al avance de la sociedad de la información y que este derecho se deriva en gran parte de las innovaciones tecnológicas; la protección de datos surge con el propósito de garantizar a las personas un control sobre el tratamiento de datos no solo de carácter personal, de la misma forma, trata de garantizar control sobre el tratamiento de cualquier otro tipo de dato.

Otro concepto formulado por Remolina [10], es el de habeas data definido como la protección de los datos personales, este es un recurso y un derecho fundamental para suministrarle una herramienta al ciudadano y poder exigir a quien maneja y administra sus datos personales en entidades privadas y públicas el debido uso de

dicha información. Es decir, el derecho a conocer, a actualizar y a rectificar la información que sobre ellos reposa en cualquier base de datos. De esta forma las personas tienen el derecho de saber cómo sus datos se recolectaron, para qué serán utilizados, quién los tiene; si son erróneos o equívocos, para poder corregirlos o modificarlos.

La importancia del habeas data radica en que en la sociedad de hoy la información es el eje fundamental de las entidades para tomar cualquier decisión. Otra de las razones es que la información se ha convertido en un objeto de negocio; existen empresas que se dedican a la recolección y venta de esos datos. Frente a ello, lo que se quiere es que no exista un uso indebido de la información, de tal modo que no se afecten los derechos fundamentales de la persona, como son la intimidad, el buen nombre entre otros. La regulación del habeas data no es para impedir el tratamiento de los datos personales, su propósito es que la información se administre de forma adecuada.

Una clasificación de los diversos tipos de habeas data fue propuesta por Sagües [11], los cuales se presentan en la Tabla 2.

Tabla 2. Tipos de habeas data

Tipos de habeas data	Definición
Habeas data informativo	Cuando se utilice para acceder a la información que se tiene sobre si en una determinada base de datos.
Habeas data aditivo	Aquel que trata de actualizar o incluir datos o información dentro de los archivos.
Habeas data rectificador o correctivo	Cuando se corrige informaciones falsas, inexactas o imprecisas.
Habeas data reservador	Su objetivo es asegurar que un dato determinado sea proporcionado a quienes se encuentran legalmente autorizados para conocerlo.
Habeas data exclutorio o cancelatorio	Cuando se elimina información almacenado en algún banco de datos o sistema de información, posee relevancia para la información considerada sensible.

2.2 MARCO METODOLÓGICO

En esta parte se presentan los conceptos de la metodología utilizada para desarrollar el proyecto de investigación y los mecanismos para recolectar la información.

2.2.1 Metodología de sistemas blandos

La Metodología de los Sistemas Blandos (MSB) fue propuesta por Peter Checkland a principios de los años setenta, la cual consiste en un proceso sistémico de indagación que se orienta en un grupo de principios organizados, guiando la acción que se debe llevar a cabo para tratar de administrar situaciones problemas del mundo real, con un alto componente social, político y humano, intentando cambiar favorablemente dichas situaciones, haciendo uso de los modelos de sistemas. Esta clase de problemas que son difíciles de definir y se enfrentan a situaciones desordenadas y mal estructuradas, se denominan "problemas suaves". Sin embargo, existe otra clase de problemas, que tienen una estructura fácilmente identificable y se les da mayor importancia a la parte tecnológica en contraste con la parte social; a esta clase de problemas se les conoce como "problemas duros".

La forma básica de la metodología consta de cuatro estadios, como lo muestra la Figura 2 del capítulo uno, y a continuación se hará una descripción de cada uno de ellos. En una primera instancia, Checlankd [12] plantea que se deben hacer hallazgos acerca de una situación en el mundo real que haya generado interés. En este estadio muestra lo que el observador o los observadores perciben de la situación problema, que va acompañada de una descripción detallada a través de imágenes y diagramas (visión o imagen enriquecida), de la estructura, los procesos de comunicación, las propiedades emergentes[6] que lleva consigo la

[6] Desde la perspectiva sistémica las *«propiedades emergentes»* son propiedades del todo que ninguna de las partes posee, *«emergen»* de las interacciones y relaciones entre las partes.

situación problema. Esta visión enriquecida contribuye a una mayor comprensión del problema y del contexto de la situación.

En un segundo estadio, se seleccionan los sistemas pertinentes, para ello, primordialmente es necesario nombrarlos a través de las Definiciones Raíces (DR), las cuales son una descripción de un grupo de actividades con propósito definido, en las que se realiza un proceso de transformación deseable para la situación problema. Las DR especifican las personas involucradas en la transformación, las que llevan a cabo esta transformación, las que limitan la situación problema, el punto de vista que se tiene en cuenta, los recursos y restricciones de la situación. Para que las DR queden bien formuladas, los investigadores pueden hacer uso del mnemónico CATWOE, el cual se especifica a continuación en la Tabla 3.

Tabla 3. Descripción de los elementos del CATWOE

Elementos del CATWOE		
Sigla	**Elemento**	**Descripción**
C	**Cliente**	Son los beneficiarios o victimas afectados por la transformación.
A	**Actor**	Los actores realizan las actividades o transformación en el sistema.
T	**Transformación**	Es el núcleo de la definición raíz, consiste en un proceso que convierte un conjunto de entrada de información en un conjunto de salida.
W	**Weltanschauung**	Opinión del mundo que hace que la transformación sea significativa en el contexto que se está modelando, es decir la interpretación del propósito de la transformación.
O	**Propietario**	Quien tiene el poder de comenzar, cerrar el sistema o detener la transformación.
E	**Restricciones**	Elementos fuera del sistema que este toma como dados.

Una vez establecidas las DR se procede a modelar el Sistema de Actividades Humanas (SAH), el cual es un grupo estructurado de verbos, que describen las actividades necesarias y requeridas en el sistema, definidas en las DR, y deben

estar conectadas entre si constituyendo un todo con un propósito definido. Además, se hace necesario resaltar que, cada frase en la DR está unida a actividades y conexiones particulares en el modelo y se debe demostrar que cada aspecto del modelo deriva de las palabras en la definición.

En el tercer estadio, se usan los modelos conceptuales diseñados en el segundo estadio, para cuestionar la situación del mundo real, ilustrada en las imágenes enriquecidas, realizando de esta manera una fase de comparación. Checkland [12] determina cuatro formas de llevar a cabo esta comparación: discusión informal, cuestionamiento formal, escritura acerca del escenario basada en la "operación" de los modelos, e intento por modelar el mundo real bajo la misma estructura que tienen los modelos conceptuales, sin embargo la opción más utilizada es el cuestionamiento formal, que se basa en un debate entre los modelos conceptuales y la situación problema. Cabe anotar, que el propósito de este estadio no es mejorar los modelos en una fase de comparación, sino encontrar un acomodo entre los diferentes intereses en la situación, que se pueda argumentar para construir así una mejoría en la situación problema inicial.

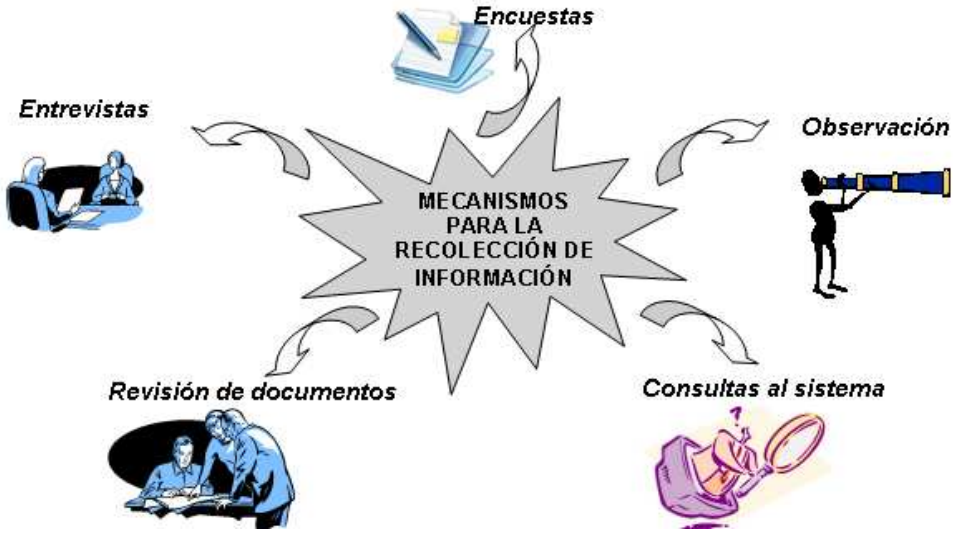
Según Checkland [12], en el cuarto estadio se utiliza el debate iniciado anteriormente en la comparación, para identificar y llevar a cabo cambios que puedan mejorar la situación problema, los cuales deben ser evaluados y aprobados por las personas que han contribuido en el estudio de ésta. Dos características fundamentales de estos cambios según lo propuesto por Checkland, son: la primera, es que los cambios deben ser deseables sistémicamente, es decir, que los cambios no se deben tomar como forzosos sino como deseables, demostrando que los modelos de sistemas de actividades elegidos, son pertinentes a la situación problema; y la segunda, es que los cambios deben ser viables culturalmente, es decir, que se consideren significativos en la cultura establecida de la situación estudiada. Es importante anotar, que este estadio no representa el fin de la aplicación de la metodología,

pues en su aplicación se transforma en un ciclo de continua conceptualización y habilitación de cambios, siempre tendiendo a mejorar la situación problema.

2.2.2 Mecanismos para la recolección de información

Para conocer el tratamiento de los datos personal en el sistema de información de una organización, este proyecto ha definido los mecanismos necesarios para la recolección de información basados en Kendall [13] y Senn [14] (Ver Figura 5), los cuales son: entrevistas, encuestas, consultas al sistema, observación y revisión de documentos. Con la ayuda de estos mecanismos se conocerá el nivel de cumplimiento de los derechos de protección de datos que tendrá un sistema de información. A continuación, se presentará una descripción de los mecanismos de recolección de información, mostrando cuando es necesario utilizarlos en la aplicación del modelo propuesto:

Figura 5. Mecanismos definidos para la recolección de la información.



- **Entrevistas:** este mecanismo se emplea para conocer los objetivos, los procedimientos informales, el estado actual de una organización; la manera como se administran los sistemas de información y ayuda a comprender la cultura de la organización.

- **Encuestas:** este mecanismo lo aplica la organización para extraer datos críticos y recolectar información sobre la administración del sistema de información desde el punto de vista del usuario. A demás, este puede ser útil para verificar la información recolectada en la entrevista.

- **Consultas al sistema:** en este caso, la organización utiliza las consultas al sistema para verificar la entrada, almacenamiento, procesamiento y salida de la información.

- **Observación:** se aplica para observar a las personas que interactúan con el sistema de información de la organización, la cual pretende identificar lo que estas personas hacen, como lo hacen, cuanto tiempo toma y porque se hace. Además este mecanismo ayuda a confirmar o negar lo que ha sido encontrado por medio de entrevistas y encuestas.

- **Revisión de documentos:** a través de este mecanismo de recolección, se comprueba el estado en que se encuentra la organización y permite verificar la información recolectada por medio de entrevistas y encuestas. La revisión se podrá realizar en documentos físicos o magnéticos. Según Senn [14], esta técnica tiene 2 puntos de vistas:
    - El investigador debe examinar los documentos materiales proporcionados. Estos datos pueden ayudar a esclarecer los problemas existentes. Sin embargo los datos obtenidos deben ser verificados con otra técnica de recopilación de datos.
    - Esta técnica se enfoca en el documento específico, formas o registros utilizados en un proceso, permite examinar que datos están disponibles y en que forma, para una actividad especifica de la operación.

3. ANÁLISIS DE LAS LEYES DE PROTECCIÓN DE DATOS A NIVEL INTERNACIONAL Y NACIONAL

Este capítulo expone los documentos bases que reglamentan las legislaciones de protección datos en los diferentes países, los cuales han sido emitidos por organismos internacionales encargados de proteger los derechos humanos de las personas, como son el Concejo de la Unión Europea, la Asamblea General de la ONU y la Organización para la Cooperación y el Desarrollo Económico (OECD), de igual forma, se expondrán las leyes de protección de datos americana y europeas , lo cual permitió determinar cómo está el panorama mundial en este tema, posteriormente se presenta el análisis realizado por los autores de este trabajo de investigación de la ley 221/07 sobre el derecho de habeas data en Colombia, que permitió determinar los derechos de protección de datos que el modelo diseñado evaluará.

3.1 FUNDAMENTOS CONCEPTUALES PARA LA LEGISLACIÓN DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS

Desde la década de los sesenta se ha desarrollado un interés creciente por los derechos de protección de datos personales, lo cual ha generado que se elaboren diferentes documentos internacionales, estos se componen por principios que tienen como fin proteger estos derechos y algunos derechos fundamentales dentro del contexto de la sociedad de la información y el avance tecnológico.

Los siguientes documentos se han constituido en las bases fundamentales de numerosas legislaciones de países del mundo. Muchos de estos países han seguido los modelos originados en la Resolución 45/95 de 1990 de la ONU, al igual que los modelos del enfoque europeo, con la Directiva 95/46/CE[7].

[7] Como es el caso de los países de Austria, Bélgica, Dinamarca, Finlandia, Francia, Alemania, Grecia, Italia, Luxemburgo, Portugal, España, Suecia, Reino Unido, Argentina, Chile, Canadá, entre otros.

Según Remolina [15], dentro del contexto internacional a grandes rasgos se destacan los siguientes acuerdos y declaraciones emitidos por organizaciones internacionales en materia de protección de datos (Ver Tabla 4).

Tabla 4. Resumen de documentos bases para la legislación de derechos de protección de datos

Documento	Elaborado por	Finalidad
Resolución 509 de 1968	**Asamblea del Consejo de Europa**	Trata de los derechos humanos y los nuevos logros científicos y técnicos.
Resolución 3384 del 10 de noviembre de 1975[8]	**Asamblea General de la ONU**	Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad.
Guía para la protección de la privacidad y transferencia flujos de información personal. 23 de noviembre de 1980[9]	**Organización para la Cooperación y el Desarrollo Económico (OCDE)**	Regula la protección de la privacidad y los flujos transfronterizos de datos personales.
Convención Nº 108. Suscrita en Estrasburgo el 28 de enero de 1981[10]	**Consejo de Europa**	Protección de la personas respecto al tratamiento automatizado de datos de carácter personal.
Resolución 45/95 del 14 de diciembre de 1990[11]	**Asamblea General de las Naciones Unidas - ONU**	Principios rectores para la reglamentación de ficheros de datos personales.
Directiva 95/46/CE del 24 de octubre de 1995[12]	**Parlamento Europeo y Consejo de La Unión Europea**	Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
Directiva 97/66 CE del 15 de diciembre de 1997[13]	**Parlamento Europeo y del Concejo**	Tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones.
Carta de Derechos Humanos del 7 de	**Unión Europea**	Reforzar la protección de los derechos fundamentales, dotándolos

Para consultar la implementación de la Directiva 95/45/CE en países de Europa, visitar la página Web: http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

[8] Consultar en http://www.unhchr.ch/spanish/html/menu3/b/70_sp.htm

[9] Consultar la página Web de la OCDE en ingles: http://www.oecd.org/document/26/0,2340,en_2649_34255_1814170_1_1_1_1,00.html (Visitada en abril 2007).

[10] Consultar la página Web del Consejo de Europa: http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG (Visitada en abril 2007).

[11] Adoptada en la 68ª sesión plenaria. Consultar su contenido en http://www.un.org/spanish/documents/ga/res/45/list45.htm

[12] Publicado en: Diario Oficial L 281 de 23 de noviembre de 1995. página del parlamento europeo.

[13] Publicado en: Diario Oficial L 24/1 de 30 de enero de 1998.

Documento	Elaborado por	Finalidad
diciembre de 2000		de mayor presencia, a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos.
Directiva 2002/58/CE, del 12 de julio de 2002[14]	**Parlamento Europeo y del Consejo**	Tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones electrónicas.
Directiva 2006/24/CE 15 de marzo de 2006[15]	**Parlamento Europeo y del Consejo**	Conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

3.2 LEYES DE PROTECCIÓN DE DATOS

Las primeras leyes de protección de datos personales frente al tratamiento automatizado de los datos empiezan a surgir en los años setenta, en la actualidad todos los estados que integran la Unión Europea disponen de estas leyes, y en América ya hay varios países que las han adoptado, o están en proceso de adoptarlas; igualmente existen países en Asía y Oceanía que regulan estas leyes, se trata de un proceso normativo que continuamente avanza en todos los países del mundo, y cuya evolución está asociada a la desarrollada capacidad de almacenamiento, manejo y recuperación de información contenida en los sistemas informáticos, así como al generalizado uso de las telecomunicaciones y el procesamiento de datos.

A continuación, se presenta un estudio comprendido entre los meses de septiembre y noviembre del 2007, realizado en los países de los continentes de Europa y América, el cual tuvo como fin recopilar las normas de cada país, en lo que respecta al tratamiento automatizado de datos. La Tabla 5 muestra los artículos constitucionales de España y Portugal.

[14] Publicado en: Diario Oficial L 201 de 31 de julio del 2002.
[15] Publicado en: Diario Oficial L 105 de 13 de abril del 2006.

Tabla 5. Normalización de protección de datos en artículos constitucionales por países europeos

País	Artículo Constitucional	Descripción
ESPAÑA	Constitución Española (CE) de 1978, artículo 18.4	Este artículo establece el principio "*La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". Esta protección se cumple en el ámbito de la automatización de la información sobre los datos personales y familiares, ante la preocupación de un posible abuso en la utilización de las nuevas tecnologías.
PORTUGAL	Constitución de Portugal del 25 de abril de 1976, Artículo 35	Protege a nivel constitucional el derecho a la autodeterminación informativa, proporcionando a todo ciudadano el acceso a la información que, de ellos haya en las entidades públicas o privadas, exigiendo su rectificación o actualización, así mismo prohíbe el acceso de terceros a los datos personales y el flujo de datos transfronterizos.

En la Tabla 6, se muestran las leyes de protección de datos con respecto al tratamiento automatizado de datos personales en los países europeos.

Tabla 6. Leyes de protección de datos en Europa

País	Ley / Decreto	Descripción
ALEMANIA	**La Datenschutz, ley sobre tratamiento de datos personales del Land de Hesse**[16], promulgada el 7 de octubre de 1970, última modificación el 6 de noviembre de 1986.	Maneja registros automáticos y manuales del sector público y privado. Regula el derecho de acceso; establece la adopción de medidas de seguridad pertinentes para informar al ciudadano acerca del registro de sus datos, establece un organismo de control.
	Ley Federal alemana de protección de los datos (Bundesdatenschutzgesetz, BDSG)[17], promulgada el 27 de febrero de 1977 y entro en vigor el 1 de enero de 1978.	Reglamenta el derecho de bloqueo, normaliza infracciónales asociadas al tratamiento de datos, impone a los entes que procesen datos la adopción de medidas técnicas y de organización necesarias para garantizar la observancia de la ley.
AUSTRIA	**Ley Federal de Datos (Federal Data Act)**[18]**,**	Normaliza el derecho fundamental a la protección de datos, frente a los

[16]Muñoz De Alba Medrano, Marcia, "Derecho a la privacidad en los Sistemas de Información pública" Estudios en homenaje a Don Manuel Gutiérrez de Velasco, México, UNAM, Instituto de Investigaciones Jurídicas, 2000, p 6.
[17]Ley publicada DO CE No. L 281
[18]Publicada en la Gaceta Oficial Federal (Bundesgesetzblatt) No. 565/1978.

País	Ley / Decreto	Descripción
	promulgada el 18 de agosto de 1978.	registros públicos y los privados, en particular los datos que respectan la vida privada y familiar. En cuanto a los datos nominativos*, éstos sólo pueden obtenerse cuando se trate de bancos públicos de datos; se creó la Comisión de Protección de Datos con facultades de índole administrativa y judicial.
BELGICA	**Ley sobre Privacidad[19],** promulgada el 8 de diciembre de 1992.	Reglamenta la protección de la vida privada respecto a los tratamientos de datos de carácter personal.
DINAMARCA	**Ley N º 429, sobre protección de datos personales**, 31 de mayo de 2000[20].	Protege los datos personales automatizados y los que hacen parte de un sistema de archivo o estén destinados a formar parte de un sistema de presentación, de manera total o parcialmente.
ESPAÑA	**Ley Orgánica 5/1992**, del 29 de octubre, De Regulación Del Tratamiento Automatizado De Los Datos De Carácter Personal (LORTAD)[21].	Tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos. Su ámbito de aplicación se circunscribe a los ficheros de carácter automatizados.
	Real Decreto 1332, promulgado el 20 de junio de 1994[22]	Desarrolla determinados aspectos de la ley orgánica 5/1992, de 29 de octubre que corresponden a los artículos 2.3, 3, 47, transferencia internacional de datos, notificaciones e inscripción de ficheros, ejercicio y tutela de los derechos del afectado.
	Ley Orgánica 15/1999, sobre Protección de Datos de Carácter Personal “LOPD” (substituye a la LORTAD), promulgada el 13 de diciembre[23]	Reglamenta los derechos fundamentales de las personas, en especial el derecho al honor y a la intimidad personal y familiar, respecto al tratamiento de los datos de carácter personal. Establece un organismo encargado de controlar el cumplimiento de las disposiciones de la citada ley.

* Aquellos datos que permiten revelar la identidad de una persona.
[19]Publicada en el Diario Oficial, 3 de febrero de 1999.
[20]Publica en "Lovtidende" (Diario Oficial), el 2 de junio de 2000.
[21]Publicada el 31 de octubre de 1992, en el B. O. E. Número 262.
[22]Decreto publicado el 21 de junio de 1994, en el B. O. E. Número 147.
[23]Publicada el 14 de diciembre de 1999, en el B. O. E. Número 298.

País	Ley / Decreto	Descripción
	Real Decreto 994, promulgada el 11 de junio de 1999[24]	Establece y desarrolla el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal de los artículos 9 y 43.3.h de la Ley Orgánica 5/1992, de 29 de octubre.
FRANCIA	**Ley 78-17 relativa a la informática, los ficheros y las libertades**, 6 de enero de 1978[25] (Informatique, aux Fichiéres et aux Libertés)	Reglamenta el tratamiento automatizado de datos personales públicos y privados, referidos a personas físicas, realizado por personas naturales o jurídicas, admite la aplicación parcial de sus disposiciones al tratamiento manual de datos nominativos. Además, posee un ámbito de aplicación que cubre la totalidad de los sectores de actividad, ficheros en el campo de la seguridad pública, la defensa, y materia penal.
GRECIA	**Ley 2472/97 sobre la protección de las personas con respecto al tratamiento de datos de carácter personal**[26], promulgada el 10 de abril de 1997.	Establece los términos y las condiciones de tratamiento de los datos personales a fin de proteger los derechos y libertades fundamentales de las personas naturales, especialmente en relación con la intimidad.
HUNGRIA	**Ley LXIII, de 1992, sobre la protección de los datos personales y la publicidad de los datos de interés público (en adelante Ley de protección de datos)**[27]. Promulgada el 17 de noviembre de 1992 y entró en vigor el 1 de mayo de 1993,	Garantiza la protección de la dignidad humana y el libre desarrollo de la personalidad, mediante un marco legal que restringe el derecho a la libre determinación en materia de información, y la publicidad de los datos de interés público. Además estableció la institución del Defensor del pueblo para los Derechos de las Minorías Nacionales y Étnicas.
IRLANDA	**Ley de Protección de Datos Personales**[28], sancionada el 13 de julio de 1988.	Establece disposiciones para la recolección, tratamiento, mantenimiento, uso y divulgación de cierta información relativa a las personas que se procesan automáticamente, aplicando un sistema selectivo que obliga a registrarse anualmente a los principales responsables del tratamiento de datos.
	Ley de Protección de Datos[29]**,** promulgada el 10 de	Referente a la protección de las personas físicas con respecto al

[24]Decreto publicado el 25 de junio de 1999, en el B. O. E. Número 151.
[25]Ley publicada en la Comisión Nacional de Informática y Libertades (CNIL), Francia, 27 de enero del 2006.
[26]Publicada el 24 de 1997, Boletín Oficial A-50.
[27]Publicada en el Diario Oficial N°L 215 de 25/08/20 00 p. 0004 – 0006.
[28]Publicada en el B. O. Número 25 de 1988.
[29]Publicada en el B. O. Número 6 del 2003.

País	Ley / Decreto	Descripción
	abril 2003.Reforma de la ley de protección de datos 1988.	tratamiento de datos personales y sobre la libre circulación de estos datos.
ITALIA	**Ley 675, sobre la tutela de las personas y otros sujetos respecto al tratamiento de datos personales,** del 31 de diciembre de 1996[30]. Entró en vigor el 8 de mayo de 1997.	Establece que datos de carácter personal facilitados por el usuario podrán ser objeto de tratamiento con finalidades administrativas, técnicas, productivas y estadísticas, mediante la consultación, elaboración, comparación, comunicación y cualquier otra operación tratamiento que sea considerada oportuna.
LUXEMBURGO	**Ley de 2 de agosto de 2002** sobre la protección de las personas con respecto al tratamiento de datos personales[31].	Relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y garantiza el respeto de los intereses legítimos de las personas jurídicas.
NORUEGA	**Ley N° 48, sobre registro de datos personales**[32]. Sancionada el 9 de junio de 1978. Entró en vigor el 1º de enero de 1980.	Se establece para todo tipo de registros, es decir, automatizado o manual, público o privado, y deben contar tanto con la autorización previa de funcionamiento, para tratar información sensible y transferir los datos transfrontera. Además se crea el organismo" inspección de Datos" que tutela, entre otras cosas los datos personales.
PORTUGAL	**Ley No. 10, sobre protección de datos personales frente a la informática** del 19 de febrero de 1991[33], promulgada el 9 de abril de 1991.	Se expidió a nivel reglamentario como efecto de ampliar los parámetros de la Constitución, creando así la Comisión Nacional de Protección de Datos Personales Informatizados, autoridad responsable y encargada de la correcta aplicación de estos ordenamientos y establece los requisitos para el tratamiento de la información sensible.
	Ley No. 67, de protección de datos, del 26 de Octubre de 1998[34]. Entró en vigor el 24 de septiembre de 1998.	Relativa a la Protección de Datos de Carácter Personal y a la libre circulación de estos datos. Además establece como principio general que el tratamiento de los datos personales debe hacerse de manera transparente y dentro del estricto respeto a la preservación de la vida privada, así como de los derechos, las libertades y las garantías

[30]Publicada en la Gazzetta Ufficiale della Repubblica Italiana n°5, suplemento 3, de 1997.
[31]Ley publicada en el Diario Oficial the Grand Duchy of Luxembourg, Compendio de la legislación Número 91, 13 de agosto de 2002
[32]Muñoz De Alba Medrano, Marcia, op. cit., nota 1, p 7.
[33]Publicada en Diario da República, Nº 98, 29 de abril de 1991, págs. 2366-2372
[34]Publicada en Diario da República, Nº 247, 26 de Octubre de 1998, págs. 5536-5546.

País	Ley / Decreto	Descripción
		fundamentales.
SUECIA	**Data Act,** del 11 de mayo de 1973[35]. Entró en vigor 1º de julio de 1974.	Sitúa en posición de igualdad tanto al funcionario público como al ciudadano respecto al acceso a la información. Obliga a registrar los archivos electrónicos de datos personales de carácter público o privado y establece la obtención de licencias para gestionar los datos personales; además para los datos personales sensibles se hace necesaria la autorización de la Inspección de Datos, órgano encargado de la aplicación de la Ley.
	Ley 1998/204 sobre Protección de Datos de Carácter Personal[36].Entró en vigor el 24 de octubre de 1998.	Modificó el artículo 33 de dicha Ley (transferencia a terceros países), de modo que la adaptación a la Directiva fuera más estricta. El nuevo artículo 33 establece que los datos personales sólo se pueden transferir a terceros países donde el nivel de protección sea adecuado. También prevé las circunstancias que se deben tener en cuenta para evaluar si el nivel de protección es adecuado.

En la Tabla 7, se muestran los países americanos que poseen artículos constitucionales con respecto al derecho de protección de datos personales.

Tabla 7. Normalización de protección de datos en artículos constitucionales por países Americanos

País	Artículo Constitucional	Descripción
Argentina	Constitución de la Nación Argentina de 1.994, artículo 43	Establece el derecho que toda persona tiene a exigir la supresión, rectificación, confidencialidad, actualización de datos a ella referidos, en caso de falsedad o discriminación.
Brasil	Constitución Política de la República Federativa de 1988, artículo 5 incisos: X, XII y LXXII).	Establece a todas las personas, el respeto y protección a la vida privada y pública, a la honra de la persona y de su familia, la inviolabilidad de las comunicaciones y el habeas data.
Colombia	Constitución Política de la República de Colombia de 1991, artículo 15	Establece el derecho a la intimidad personal y familiar, el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido

[35]Muñoz De Alba Medrano, Marcia, op. cit., nota 1, p 6.
[36]Guía de trabajo sobre protección de datos, WP 46(5019/02/ES), 17 de mayo de 2001.

País	Artículo Constitucional	Descripción
		sobre ellas en bancos de datos.
Ecuador	Constitución Política de la República del Ecuador de 1998, artículo 94	Regula el habeas data, dentro de los cuales establece el derecho a la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.
Guatemala	Constitución Política de la República de Guatemala de 1985, artículo 31	Regula el acceso a archivos y registros estatales, las cuales establecen el derecho a la corrección, rectificación y actualización de datos personales, de igual manera declara el derecho a conocer la finalidad de sus datos.
Nicaragua	Constitución Política de la República de Nicaragua 1987, artículo 26 ítem 4	Normaliza que toda persona tiene derecho a: "*conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información*".
Paraguay	Constitución de la República de Paraguay de 1992, artículo 135	Este artículo reglamenta el habeas data.
Perú	Constitución Política del Perú de 1994. artículo 2 y 200	Estos artículos establecen el derecho a que los servicios informáticos, no suministren informaciones que afecten la intimidad personal y familiar; y establece la garantía constitucional del habeas data.

En la Tabla 8, se muestran las leyes o decretos de protección de datos establecidos en los países de América.

Tabla 8. Leyes de protección de datos en América

País	Ley / Decreto	Descripción
Argentina	**Ley 25.326, Ley de Protección de Datos Personales**. Promulgada parcialmente el 30 de Octubre del 2000[37]	Regula la protección de los datos personales, para garantizar el derecho a la intimidad de las personas, y el derecho a tener acceso a la información que sobre ellas se registre.
	Decreto 995/2000, Número 29517 [38]	Anula los artículos 29, puntos 2 y 3, en lo referente al Órgano de Control y el artículo 47, en lo que concierne a eliminar datos referidos al incumplimiento de una obligación, si esta ha sido cancelada al momento de la entrada en vigencia de la ley 25326.
	Decreto 1558/2001 Número	Aprueba la reglamentación de la ley 25.326.

[37] Ley publicada el 21 de noviembre del 2000 en el Boletín Oficial de Argentina, Numero 1074
[38] Publicado en el Boletín Oficial del 2/11/2000, Número 29517

País	Ley / Decreto	Descripción
	29787 [39]	Principios generales relativos a la Protección de Datos Personales. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones.
Brasil	**Ley 9.507,** publicada el 12 de noviembre de 1997.	Regula el derecho a la información pública y reglamenta el habeas data.
Chile	**Ley 19.628**, **Ley Protección de Datos de Carácter Personal,** promulgada el 18 de agosto de 1999[40]	Regula el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares.
	Decreto 779/2000, promulgada el 24 de agosto del 2000[41]	Aprueba reglamento del Registro de Bancos de Datos Personales a cargo de organismos públicos de la ley 19628.
	Ley 19.812, promulgada el 11 de junio de 2002, que modifica la ley 19628.[42]	Dentro de las modificaciones, reglamentada un precepto en el Código del Trabajo; regula la eliminación de los registros históricos de obligaciones financieras, una vez aclarada la morosidad; regula la reserva de las recetas médicas.
Colombia	**Ley 221/07, Ley sobre el derecho de Habeas Data en Colombia**, en proceso de aprobación por parte de la Corte Constitucional.	Establece las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ecuador	**Ley de Control Constitucional**, artículos del 34 al 45[43]	Estos artículos comprenden el capítulo II que regulan el habeas data.
México	**Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental**, artículos 20 al 26[44]	Estos artículos comprenden el capítulo 4, el cual regula la protección de datos personales, en el que proporciona el acceso y la corrección de la información de carácter personal.
Panamá	**Ley 6**, promulgada el 22 enero de 2002[45]	Dicta normas que establece la acción de habeas data, y otras disposiciones.
	Ley 24, promulgada el 22 de mayo de 2002[46]	Regula la confiabilidad, la veracidad, la actualización y el buen manejo de los datos personales de consumidores o clientes, relativos a su historial de crédito.

[39] Publicado en el Boletín Oficial del 3/12/2001, Numero 29787
[40] Ley publicada el 28 de Agosto del 1999 en el Boletín Oficial de Chile
[41] Decreto publicado en el D. O. el 11/11/2000
[42] Ley publicada en el Diario Oficial de Chile el 13/06/2002
[43] Publicada en el Registro Oficial 99 de 2 de Julio de 1997
[44] Ultima reforma publicada el 11/05/2004 en el Diario Oficial de la Federación
[45] Publicada en la Gaceta Oficial Nº 24.476 de 23 de enero de 2002
[46] Publicada en la Gaceta Oficial Nº 24.559 de 24 de mayo de 2002

País	Ley / Decreto	Descripción
Paraguay	**Ley 1.682,** sancionada el 28 de diciembre del 2000[47]	Reglamenta la información de carácter privado, la cual establece la acción de habeas data, delimita los datos sensibles.
	Ley 1.969, que modifica la ley 1.682, sancionada el 22 de agosto del 2002[48]	Regula en general el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares. Modifica y amplia los artículos 1, 2, 5, 7, 9 y 10 de ley 1.682.
Perú	**Ley 27.489** promulgada el 28 de junio del 2001, artículos 9 al 18[49]	Regula las Centrales Privadas de información de riesgos y de protección al titular de la información, que dentro de las cuales reglamenta la recolección, tratamiento, difusión y seguridad de información de riesgos; regula sobre el deber de seguridad de la información, sobre el derecho de los titulares de la información.
Uruguay	**Ley 17.838**, promulgada el 1º de octubre del año 2004[50]	Regula la protección de datos personales para ser utilizados en informes comerciales y acción de habeas data, por medio del cual reglamenta el tratamiento de datos personales asentados en archivos, bases de datos u otros medios similares autorizados, sean públicos o privados, destinados a brindar informes objetivos de carácter comercial.

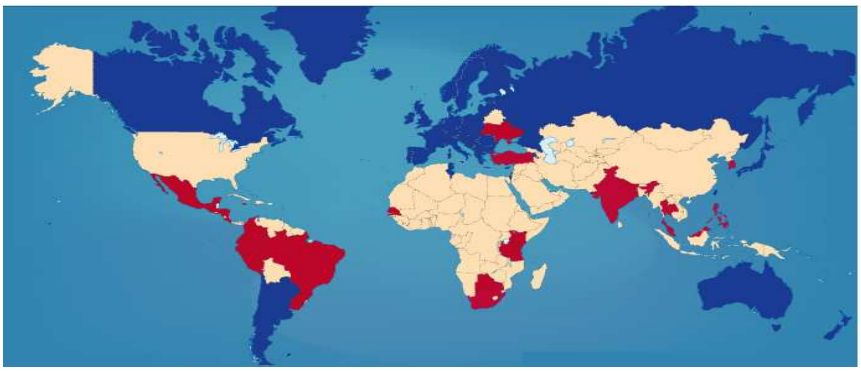
3.3 PANORAMA MUNDIAL DE LAS LEYES DE PROTECCIÓN DE DATOS

El siguiente mapa elaborado por David Banisar señala a nivel mundial los países que hasta mayo del 2007 cuentan con leyes en materia de protección de datos[51], de igual manera se señalan aquellos que se encuentran en proceso de elaboración de dicha ley; como es el caso de Colombia y otros países sur americanos, y además muestra aquellos países que no cuentan con una norma que regule este derecho.

[47] Ley promulgada en 16/01/2001 y publicada el 19/01/2001
[48] Esta ley fue promulgada en 03/09/2002 y publicada el 06/09/2002
[49] Publicada en el diario Oficial "El Peruano" el 28/06/2001.
[50] Publicada D.O. 01/10/2004 – N°26599
[51] Publicado en: http://www.privacyinternational.org/ o http://www.privacyinternational.org/survey/dpmap.jpg

En la Figura 6, se puede observar que Estados Unidos[52] al igual que gran parte de los países de África y el medio oriente, no han establecidos normas obligatorias de protección de datos personales informatizados; a diferencia de países en vías de desarrollo como la India o Centroamérica, que se encuentran en vía de adaptarse a una legislación formal en materia de protección de datos.

Figura 6. Panorama mundial de leyes de protección de datos



Fuente: Privacy Internacional, 2007.

Azul: Ley de protección adecuada y completa.

Rojo: Esfuerzos pendientes por implementar leyes.

Beige: No tiene ley general para la protección de datos.

3.4 LEY DE PROTECCIÓN DE DATOS EN COLOMBIA

En Colombia la Constitución Política establece varios artículos concernientes al derecho de información como un derecho fundamental de las personas, como son

[52] El caso de Estados Unidos es muy particular, en el mapa este no aparece con una ley de protección de datos establecida, ya que su legislación es sectorial y no es de obligado cumplimiento, como si lo es para la Unión Europea y el resto de países que implementan este tipo de leyes, además la Directiva de Datos de la Unión Europea que entró en vigor en octubre de 1998, restringe el flujo de cualquier información a otros países que no posean un nivel adecuado de protección de datos, como es el caso de Estados Unidos que no cumple con las leyes europeas en materias de información personal; sin embargo, para que las empresas de los Estados Unidos puedan realizar transacciones de datos hacia la Unión Europea, el Departamento de Comercio de los Estados Unidos y la Comisión Europea desarrollaron el acuerdo marco "Safe Harbor" o "Puerto Seguro", las empresas que hacen parte de este acuerdo se auto-certifican que cumplen con los estándares de la Directiva Europea y que posee un nivel "adecuado" de protección a la intimidad, esto lo hacen de manera totalmente voluntaria ante el Departamento de Comercio de los Estados Unidos, de lo contrario no podrán realizar transacciones de datos de carácter personal con los países pertenecientes a la Comunidad Europea.

los artículos 15[53], 20[54] y 74[55]; en Colombia aún no se cuenta con una ley de protección de datos, no obstante después de varios intentos por aprobar una ley de protección de datos, la Ley 221/07 Derecho de habeas data en Colombia, fue aprobada por el Congreso[16] en mayo de 2007, pero hasta julio del 2008, fecha en que finalizó esta investigación, esta aún no tenía vigencia[56] ya que esta Ley está a la espera de revisión por parte de la Corte Constitucional. Una vez entre en vigencia la ley, las personas que realicen actividades que esta regula, tendrán un plazo de hasta 6 meses para adecuar su funcionamiento a sus disposiciones. A continuación se procederá a presentar un resumen que destaca los aspectos más significativos de esta ley:

3.4.1 Objeto y ámbito de aplicación de la ley

La Tabla 9, presenta el objetivo por el cual será regulada la ley de habeas data en Colombia y el ámbito en el cual será aplicada esta ley, los cuales son definidos en el primer y segundo articulo de la ley respectivamente.

[53] **Artículo 15.** Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.
En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley….

[54] **Articulo 20.** Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

[55] **Articulo 74.** Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley.

[56] Por ser una Ley Estatutaria, la cual posee un rango superior a una ley ordinaria, y debido a su naturaleza especial bajo la Constitución Política de Colombia, una ley estatutaria exige ser revisada previamente por parte de la Corte Constitucional, antes de ser ley de la República y entrar a regir o aplicarse

Tabla 9. Objeto y ámbito de aplicación de la Ley

Ley 221/07 Derecho de Habeas Data en Colombia	
Objeto	Desarrollar el derecho que las personas tienen a conocer, actualizar y rectificar su información en bancos de datos, derecho a la información en particular la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
Ámbito de aplicación	Banco de datos, administrados por entidades pública o privada. Se exceptúan bases de datos de Estado por parte del Departamento Administrativo de Seguridad, DAS, y Fuerza Pública.

3.4.2 Definiciones

A continuación se mostrará en la Tabla 10, los conceptos utilizados en la Ley de habeas data en Colombia.

Tabla 10. Definiciones de la Ley de habeas data en Colombia

Definiciones	
Titular de la información	Persona a quien se refiere la información.
Fuente de información	Persona u organización que recibe o conoce datos personales de los titulares.
Operador de información	Persona u organización que recibe de las fuentes datos personales y los suministra a usuarios. Salvo que el operador sea la misma fuente de la información, este no tiene relación con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente.
Usuarios	Persona que puede acceder a la información personal de los titulares.
Dato personal	Pieza de información que puede asociarse con una persona.
Dato público	Contenido en documentos públicos relativo al estado civil de las personas.
Dato semi - privado	No tiene naturaleza intima ni pública.
Dato privado	Solo es relevante para el titular.
Agencia de información comercial	Empresa que recoge y procesa información comercial solicitada por sus clientes.
Información financiera, crediticia. Comercial y la proveniente de terceros países	Nacimiento, ejecución y extensión de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen, así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular.

3.4.3 Principios de la administración de datos

En el artículo 4º de la Ley 221/07 se definen siete principios de protección de datos de Colombia, los cuales se pueden apreciar en la Tabla 11.

Tabla 11. Principios de la administración de datos en Colombia

Nº	Principios de protección de datos en Colombia	Descripción
1	**Veracidad o calidad de los registros o datos**	La información contenida en los bancos de datos debe ser: Veraz, completa, exacta, actualizada, comprobable y comprensible.
2	**Finalidad**	La administración de datos personales debe: • Obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. Al titular se le debe informar: • La finalidad de manera previa. • Siempre que el titular solicite información al respecto.
3	**Circulación restringida**	Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados.
4	**Temporalidad de la información**	La información del titular no podrá ser: • suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos.
5	**Interpretación integral de derechos constitucionales**	Ampara los derechos constitucionales, como el hábeas data, el derecho al buen nombre, a la honra, a la intimidad y el derecho a la información.
6	**Seguridad**	La información se debe: • manejar con medidas técnicas necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado
7	**Confidencialidad**	Todas las personas que intervengan en la administración de datos personales que no tengan naturaleza de públicos están obligadas a reservar la información, inclusive después de finalizada su relación con la administración de datos.

3.4.4 Circulación de información

En el artículo 5º de la Ley de habeas data en Colombia, se define que la información personal recolectada en bancos de datos, podrá ser entregada de manera verbal, escrita o puesta a disposición de las siguientes personas y en los términos señalados, como se puede apreciar en la Tabla 12.

Tabla 12. Circulación de información de la Ley de habeas data en Colombia

Circulación de información	
La información podrá ser entregada a	Titulares o personas autorizadas.
	Usuarios de la información.
	Autoridades judiciales, previa orden judicial.
	Entidades públicas del poder ejecutivo, para cumplir con sus funciones.
	Órganos de control dependencias de investigación disciplinaria, fiscal, o administrativa, cuando la información sea necesaria en una investigación.
	A otros operadores con autorización del titular.

3.4.5 Derechos de los titulares de información

En el título II, artículo 6° de la Ley de habeas da ta en Colombia, se definen los derechos de los titulares de la información frente a los operadores de los bancos de datos, los derechos de los titulares frente a las fuentes de información y frente a los usuarios, en la Tabla 13 se muestra un resumen de estos derechos.

Tabla 13. Derechos de los titulares de la información de la Ley de habeas data en Colombia

Derechos de los titulares de información	
Frente a los operadores de los bancos de datos	Ejercer el derecho de habeas data, mediante consultas y reclamos.
	Solicitar información de los usuarios autorizados para obtener información.
Frente a las fuentes de información	Ejercer el derecho de habeas data, mediante los operadores.
	Pedir actualización de los datos en la base de datos, lo cual realizara el operador con base a la información aportada por la fuente.
Frente a los usuarios	Solicitar información sobre la utilización que los usuarios le están dando a la información.

3.4.6 Deberes de los operadores, las fuentes y los usuarios de información

Los deberes más significativos de los operadores de los bancos de datos, las fuentes de información y de los usuarios; según la Ley 221/07 derechos de habeas data en Colombia, se presentan en la Tabla 14:

Tabla 14. Deberes de administradores de bases de datos de la Ley de habeas data en Colombia

Deberes	
De los operadores de los bancos de datos	Garantizar al titular poder conocer su información y solicitar la corrección de datos.
	Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
	Impedir el deterioro, alteración, pérdida o uso no autorizado o fraudulento.
	Realizar periódica y oportunamente la actualización de los datos, cada vez que las fuentes reporten novedades.
	Tramitar peticiones, consultas y reclamos formulados por los titulares de la información.
	Indicar en el registro individual que determinada información se encuentra en discusión por parte del titular, cuando se haya presentado la solicitud de rectificación.
De las fuentes de la información	Garantizar que la información suministrada a los operadores o usuarios sea veraz, completa, exacta, actualizada y comprobable.
	Rectificar la información cuando sea incorrecta e informar a los operadores.
	Diseñar e implementar mecanismos eficaces para reportar oportunamente la información al operador.
	Solicitar la respectiva autorización otorgada por los titulares de la información, y asegurarse de no suministrar a los operadores dato cuyo suministro no esté autorizado, cuando dicha autorización sea necesaria.
	Resolver los reclamos y peticiones del titular.
	Informar al operador que determinada información se encuentra en discusión por parte del titular, cuando se haya presentado la solicitud de rectificación o actualización, para que el operador incluya en el banco de datos una mención en ese sentido hasta que finalice el trámite.
De los usuarios	Guardar reserva sobre la información que les sea suministrada por los operadores, por las fuentes o los titulares de la información y utilizar la información únicamente para los fines para los que le fue entregada.
	Informar a los titulares, a su solicitud, sobre la utilización que le está dando a la información.
	Conservar segura la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.
	Cumplir con las instrucciones que imparta la autoridad de control.

3.4.7 De los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

En el título IV de la Ley 221/07, se definen los Requisitos que deben cumplir los bancos de datos, al igual que los operadores de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países que funcionen como entes independientes a las fuentes de la información. Los requisitos especiales de funcionamiento son los mostrados en la Tabla 15:

Tabla 15. Requisitos de funcionamiento de la Ley de habeas data en Colombia

De los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países	
Requisitos especiales para los operadores	Constituirse como sociedades comerciales, entidades sin ánimo de lucro, o entidades cooperativas.
	Contar con un área de servicio al titular de la información, para la atención de peticiones, consultas y reclamos.
	Contar con un sistema de seguridad y condiciones técnicas para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado.
	Deberán actualizar la información reportada por las fuentes con una periodicidad no superior a diez (10) días.
Requisitos especiales para fuentes	Deberán actualizar mensualmente la información suministrada al operador.
	El reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los operadores de bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, sólo procederá previa comunicación al titular de la información, con el fin de que este pueda demostrar o efectuar el pago de la obligación.
Permanencia de la información	La información de carácter positivo permanecerá de manera indefinida en los bancos de datos de los operadores de información.
	Datos referentes a no cumplimiento de obligaciones, se regirán por un término máximo de permanencia, vencido el operador los retirara, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de esta información será de cuatro (4) años a partir de la fecha en que sean pagadas las cuotas la obligación vencida.
Contenido de la información	Señalar un formato que permita identificar, nombre del deudor, condición en que actúa (deudor principal, deudor solidario, avalista o fiador) monto de la obligación o cuota vencida, el tiempo de mora y la fecha del pago, si es del caso.

De los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países	
Acceso a la información por parte de los usuarios	La información podrá ser accedida por los usuarios con las siguientes finalidades: · Elemento de análisis para establecer y mantener una relación contractual. · Como elemento de análisis para hacer estudios de mercado o investigaciones comerciales o estadísticas. · Trámite ante una autoridad pública o una persona privada, si dicha información resulte pertinente.

3.4.8 Vigilancia de los destinatarios de la ley y facultades de estas entidades

La entidad que cumplirá la función de vigilancia en el cumplimiento de la Ley de habeas data en Colombia será la Superintendencia de Industria y Comercio y la Superintendencia Financiera de Colombia, según los siguientes casos (Ver Tabla 16).

Tabla 16. Función de vigilancia. Ley de habeas data en Colombia

Función de vigilancia	
Superintendencia de Industria y Comercio	Ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales.
Superintendencia Financiera de Colombia	Si la fuente, usuario u operador de información sea una entidad vigilada por la Superintendencia Financiera, esta ejercerá la vigilancia e impondrá las sanciones correspondientes.

Algunas facultades de las dos entidades anteriormente mencionadas, con respecto a la administración de datos personales financiero y crediticio, son:

- Velar porque los operadores y fuentes cuenten con un sistema de seguridad y condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros.

- Ordenar a cargo del operador, la fuente o usuario la realización de auditorías externas de sistemas para verificar el cumplimiento de esta ley.

- Iniciar de oficio o a petición de parte investigaciones administrativas contra los operadores, fuentes y usuarios de información, con el fin de establecer si existe responsabilidad administrativa derivada del incumplimiento la ley o de las órdenes y si es del caso imponer sanciones o medidas que resulten pertinentes.

3.4.9 Sanciones

En el artículo 18 de la Ley de habeas data en Colombia, se establece que los bancos de datos que no cumplan lo establecido en la Ley y administren la información de los titularles de manera incorrecta les serán impuestas las siguientes sanciones (Ver Tabla 17).

Tabla 17. Sanciones de la Ley de habeas data en Colombia

Sanciones	
Multas de carácter personal e institucional	Hasta por mil quinientos (1.500) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción, por violación a la ley de habeas data.
Suspensión de las actividades del banco de datos	Hasta por un término de seis (6) meses, cuando se estuviere llevando a cabo la administración de la información en violación grave de los requisitos previstos en esta ley.
Cierre de operaciones del banco de datos	Una vez transcurrido el término de suspensión, no hubiere adecuado su operación técnica y logística, y sus normas y procedimientos a los requisitos de ley, de conformidad con lo dispuesto en la resolución que ordenó la suspensión.
Cierre inmediato y definitivo de la operación de bancos de datos	Cuando administren datos prohibidos

3.5 ANÁLISIS DE LA LEY 221/07 DERECHO DE HABEAS DATA EN COLOMBIA FRENTE A NORMAS INTERNACIONALES.

Después de analizar algunos aspectos de la Ley y compararla con los parámetros internacionales, cabe anotar que esta aún no protege todos los derechos fundamentales de los ciudadanos en lo referente a información almacenada en medios electrónicos, sin embargo esta Ley es sólo para resolver un problema social, como es la información crediticia y financiera; además la norma se quedó

muy limitada en su alcance y no cumple con los parámetros internacionales de regulación, de igual forma ha dejado de lado aspectos tan importantes como el manejo de datos sensible; según lo anterior se podría decir que la norma es una regulación insuficiente. En la Tabla 18, se muestran las deficiencias o diferencias de la ley colombiana con respecto a otras leyes, que para resultados de este proyecto serán tenidas en cuenta.

Tabla 18. Deficiencias de la Ley de habeas data en Colombia

Deficiencias de la ley de habeas data en Colombia	
Principios que no reglamenta	
No reglamenta el principio de consentimiento	Se analizan otras leyes de protección de datos, este principio es esencial; en la ley de habeas data no se tiene en cuenta el consentimiento del titular, en su artículo 6º literal 1.4, establece que no será necesaria la autorización del titular de la información, en el caso del dato financiero y crediticio, permitiendo así que se publiquen en las bases de datos, información falsa o negativa sin que el titular se entere.
No protege información sensible	Como son los datos de la salud, religiosos, vida sexual, origen racial y étnico, filiación política datos que debe proteger cualquier norma de protección de datos.
No cumple con los reglamentos exigidos en las directivas internacionales	
Se establece un organismo de control sectorial	En el artículo 17 se establecen organismos de control sectorial, por que son dos los entes seleccionados para esta labor, en lo referente al dato financiero (Superintendencia de Industria y Comercio y la Superintendencia Financiera), por tal razón no se acoge a las exigencias de las normativas internacionales o de otros países en los que existe un ente independiente de protección de datos a nivel nacional, como por ejemplo el caso de España el órgano de control es la Agencia de Protección de Datos o en Argentina, la Dirección Nacional de Protección de Datos Personales, las cuales son independientes y poseen la suficiente capacidad para sancionar a cualquier administrador de bases de datos sin ninguna distinción, que no cumpla con la ley de protección de datos establecida.
No hay un adecuado reglamento para la transferencia internacional de datos	En el artículo 5, literal F, se trata muy por encima este tema, el mas importante internacionalmente, el cual es regulado sin control, ni garantías; porque es el operador quien decide si el tercer país o el administrador de la base de datos extranjera cumple con un adecuado nivel de protección de datos, además, esta norma no protege los datos de los ciudadanos de otros países, que si tiene leyes que regulan este tema de forma integral.
No protege completamente los derechos de protección de datos	
La ley no aplica para	Si bien es claro que la información de estas entidades no puede

Deficiencias de la ley de habeas data en Colombia	
Principios que no reglamenta	
las bases de datos del Departamento Administrativo de Seguridad-DAS y Fuerza Pública	ser de acceso a todas las personas; sin embargo esto no es excusa para que estas bases de datos no sean sancionadas por malos tratamientos, con la justificación de que manejan información para garantizar la seguridad nacional, sin tener en cuenta que pueden mantener información incorrecta de una persona a la que se le puede causar perjuicios. Sin embargo pese a esto son varios los países en donde la ley rige para todas las bases de datos en el territorio nacional, como lo dispone la Ley 25.326 de Argentina, en su artículo 44.
No hay sanción para el operador de los datos.	Según la ley colombiana, en el artículo 3 inciso C; si el operador y la fuente de información son diferentes, el operador no tiene relación con el titular y por ende no es responsable de la calidad de los datos que le sean suministrados; esto da a entender que si el operador no es quien recoge la información, este queda libre ante cualquier error en la administración de datos. Al igual que las demás leyes de protección de datos, la ley debe regir para todos los que intervengan en el tratamiento de los datos.

3.6 DERECHOS DE PROTECCIÓN DE DATOS EVALUADOS POR EL MODELO

Después del análisis realizado a la ley sobre el derecho de habeas data en Colombia, se llegó a la conclusión que esta no regula todos los principios básicos de la legislación sobre la protección de datos, además los principios que regula no lo hace de forma integral, porque esta solo es para las bases de datos que almacenan datos personales financieros y crediticios, entonces ¿qué sucede con los demás bases de datos que administran información personal?; en esta evolución de los sistemas de información, Colombia al igual que todos los países tienen la necesidad de ampliar esta ley a todas las bases de datos, sin embargo por necesidad de los sectores más sobresalientes del país como los bancos u otras entidades financieras, sólo se da un primer paso para bases de datos que almacenan información personal financiera. Por tal razón fue necesario estudiar otras normas, como por ejemplo leyes de los países de España y Argentina comparar y anexar los principios de estas al diseño del modelo para ser evaluados en un sistema de información; de esta forma el modelo diseñado es integral, acorde con la normativa internacional, con un mayor alcance que los definidos en la ley de Colombia y con las necesidades exigidas por el avance tecnológico.

El estudio realizado a varias normas permitió redefinir los derechos básicos de protección de datos personales para ser evaluados por el modelo, como se aprecia en la Tabla 19:

Tabla 19. Derechos de protección de datos a evaluar por el modelo de protección de datos

Derechos de protección de datos a evaluar por el modelo		
N	**Derechos de protección de datos**	**Descripción**
1	**Calidad de datos**	Los datos que se recojan deben ser exactos, adecuados y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido, actualizarse en caso de ser necesario y deben ser cancelados cuando hayan dejado de ser necesarios.
2	**Derecho de información en la recogida de datos**	Al solicitar datos personales, los interesados deben ser informados de la creación de la base de datos, la finalidad de la recogida de los datos y los destinatarios de la información.
3	**Consentimiento**	Para el tratamiento de datos personales es necesaria la autorización del titular de los datos, salvo excepciones de la ley.
4	**Datos sensibles**	A estos datos se le debe garantizar un tratamiento especial y solo con el consentimiento expreso del interesado podrán ser recabados datos que revelen origen racial y étnico, ideología, afiliación sindical, religión, opiniones políticas, creencias, salud, o vida sexual, al igual que comisión de infracciones penales o administrativas.
5	**Seguridad de datos**	El administrador o usuario de la base de datos debe adoptar medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales, evitando la falsificación, pérdida o consulta no autorizada.
6	**Deber de secreto**	El responsable del fichero y las personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos.
7	**Comunicación de datos o cesión**	Los datos personales sólo podrán ser comunicados a un tercero para el cumplimiento de las funciones del cedente y del receptor con el previo consentimiento del titular de los datos, e informarle a este sobre la finalidad de la cesión.
8	**Transferencia internacional**	Al transferir datos personales de cualquier tipo con otros países u organismos internacionales, el país destinatario debe garantizar y brindar niveles de protección adecuados a dichos datos.

4 DISEÑO DEL MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN

Después del análisis realizado a las leyes de protección de datos existentes en diferentes países de Europa y América; este capítulo continua con el diseño del modelo para evaluar el cumplimiento de los derechos de protección de datos en los sistemas de información, el cual se expresa en Sistemas de Actividad Humana de la Metodología de Sistemas Blandos planteada en el capítulo 2, por lo cual se presentan los hallazgos de la situación problema, el planteamiento de la definición raíz y por último se presenta el modelo de sistemas de actividades humanas, el cual describe el conjunto de actividades necesarias para llevar a cabo el objetivo planteado[57]. Sin embargo, se requiere inicialmente describir en este capítulo los componentes esenciales y los indicadores para la respetiva evaluación en los sistemas de información.

4.1 DEFINICIÓN DEL MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN

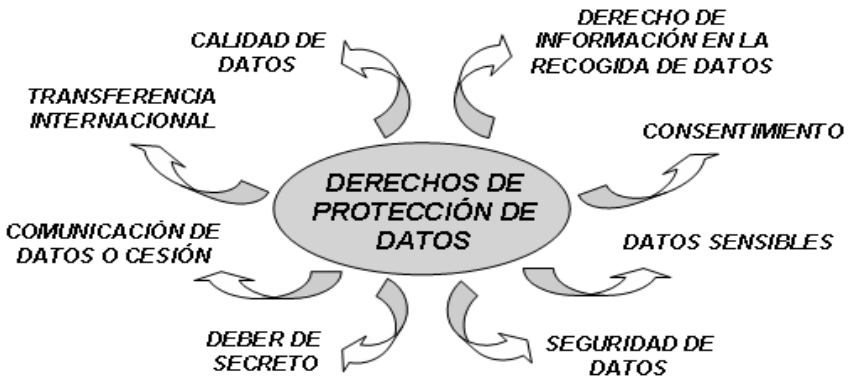
El modelo diseñado evalúa los derechos de protección de datos en las diferentes etapas del procesamiento de datos en los sistemas de información de una organización, definidas anteriormente en el capítulo 2; como son las etapas de recolección y registro de datos, procesamiento, almacenamiento y utilización de datos. A continuación se presentan los derechos de protección de datos evaluados por el modelo en cada una de las etapas definidas:

[57] El objetivo general expone lo siguiente: “definir un modelo que permita estudiar el cumplimiento de los derechos de protección de datos, evaluando los Sistemas de Información, para garantizar el derecho del habeas data, ilustrando como caso de estudio, su aplicación en la dependencia de Admisiones, Registro y Control Académico de la Universidad del Magdalena”.

4.1.1 Derechos de protección de datos evaluados por el modelo

El modelo diseñado define como variables de análisis, los derechos de protección de datos descritos en el capítulo 3, los cuales se presentan en la Figura 7; teniendo en cuenta estos derechos de protección de datos y las etapas del procesamiento de datos en un sistema de información, se realizó un análisis que permitió determinar la relación entre cada uno de estos componentes y clasificar los derechos de protección de datos a evaluar en cada una de las etapas definidas.

Figura 7. Derechos de protección de datos evaluados por el modelo.



4.1.1.1 Derechos de protección de datos a evaluar en la etapa de recolección y registro de datos

En esta etapa se evalúa que los datos recolectados y registrados en un sistema de información de una organización, sean datos de calidad (reales, completos, actualizados); igualmente si la organización o el responsable de recolectar los datos informa de manera clara y precisa al titular de estos la finalidad para la cual estos son recolectados y si se solicita su consentimiento en caso de ser necesario para registrar los datos en los sistemas; así mismo, se evalúa si estos procedimientos se llevan a cabo al recolectar y registrar en los sistemas datos sensibles. Los derechos de protección de datos a evaluar en esta etapa son:

calidad de datos, derechos de información en la recogida, consentimiento y datos sensibles.

4.1.1.2 Derechos de protección de datos a evaluar en la etapa de procesamiento de datos

Al procesar los datos se debe tener presente verificar que los controles utilizados sean eficaces para mantener la seguridad de la información, que existan los controles de accesos necesarios para que los usuarios sean fácilmente identificados y sólo personal autorizado procese información confidencial; todo lo anterior hace parte del derecho de protección de datos evaluado en la etapa de procesamiento, el cual es: seguridad de datos.

4.1.1.3 Derechos de protección de datos a evaluar en la etapa de almacenamiento de datos

Después que los datos son recolectados y registrados, estos pasan a ser almacenados en las bases de datos de los sistema de información; en esta etapa se evalúa si el administrador de la base de datos ha establecido los controles técnicos necesarios para mantener los datos almacenados, actualizados y protegidos; igualmente se evalúa el nivel de riesgo por pérdida, robo, destrucción cancelación o consulta no autorizada a la información almacenada por parte de agentes o amenazas internas o externas a la organización. Los derechos de protección de datos a evaluar en esta etapa son: calidad de datos, datos sensibles y seguridad de datos.

4.1.1.4 Derechos de protección de datos a evaluar en la etapa de utilización de datos

En esta etapa se verifica que los datos no sean utilizados para fines distintos a los determinados en el momento de la recolección, que estos no sean publicados por la organización sin previa autorización del titular, también se evalúan los controles técnicos y administrativos establecidos para conservar la seguridad de los datos al

momento de ser utilizados por el personal a cargo, lo cual incluye revisar como están distribuidas y si están documentadas las funciones y obligaciones del personal y si estos conocen las normas de seguridad y el compromiso de guardar secreto cuando tienen conocimiento o acceso a datos personales confidenciales, también se verifica que los accesos a los sistemas sean limitados a las funciones y actividades a desempeñar; por otra parte, en esta etapa se evalúan los procedimientos llevados a cabo y los controles usados al momento de ceder datos a otras áreas u organizaciones; por último se valoran los procedimientos y controles para transferir datos personales a otros países y las políticas de seguridad establecidas para tal fin. Los derechos de protección de datos a evaluar en esta etapa son: datos sensibles, seguridad de datos, deber de secreto, comunicación de datos o cesión y transferencia internacional de datos. La Tabla 20 muestra un resumen de los derechos de protección de datos a evaluar en cada una da las etapas del procesamiento de datos.

Tabla 20. Derechos de protección de datos a evaluar en cada etapa.

Etapas	Derechos de protección de datos a evaluar
Recolección y registro de datos	Calidad de datos
	Derechos de información en la recogida
	Consentimiento
	Datos sensible
Procesamiento de datos	Seguridad de datos
Almacenamiento de datos	Calidad de datos
	Datos sensibles
	Seguridad de datos
Utilización de datos	Datos sensibles
	Seguridad de datos
	Deber de secreto
	Comunicación de datos o cesión
	Transferencia internacional

4.1.2 Factores que influyen en la evaluación de los derechos de protección de datos

Después de determinar qué derechos de protección de datos se evaluarán en cada etapa del procesamiento de datos, se procede a identificar los factores que influyen en la evaluación de estos derechos, los cuales son considerados como controles, para proteger los datos de posibles abusos y riesgos en los sistemas de información; posteriormente se mostrará que estos factores están formados por una serie de interrogantes que investigan cuales de estos factores se cumplen o son tenidos en cuenta por la organización, al momento de procesar sus datos. En las Tablas 21 a 28, se describen los factores que influyen al evaluar cada uno de los derechos de protección de datos.

Tabla 21. Factores que influyen en el derecho de calidad de datos

Derecho de Protección de Datos: Calidad de los datos	
Factores	**Descripción**
Redundancia de datos	Este factor controla la presencia de datos duplicados en múltiples archivos de datos, especialmente cuando diferentes divisiones, áreas funcionales y grupos de una organización recolectan de manera independiente la misma información.
Control de entradas en campos	Este factor verifica que los datos ingresados a las base de datos para ser almacenados o procesados, sean precisos, completos e ingresados sólo una vez.
Seguimiento de la información	Es el control que se realiza a la información almacenada, procesada y utilizada, verificando que sea real, completa, actualizada y utilizada para la finalidad por la cual fue recolectada.
Actualización de datos	Este factor verifica que la información almacenada en las bases de datos sea exacta, completa, acertada y actualizada.

Tabla 22. Factores que influyen en el derecho de información en la recogida de datos

Derecho de Protección de Datos: Derecho de información en la recogida de datos	
Factores	**Descripción**
Procedimiento de recogida de datos personales	Se basa en el control de la recolección de datos personales, el cual tiene en cuenta informar de forma expresa, precisa y clara al titular de los datos de la creación de una base de datos, de la finalidad, del deber de suministrar los datos solicitados, de la posibilidad de ejercer los derechos de acceso, de rectificación y cancelación.
Documentos de soporte	En este factor se verifica si el titular proporciona sus datos de manera voluntaria a través de documentos de autorización por escritos o

Derecho de Protección de Datos: Derecho de información en la recogida de datos	
Factores	**Descripción**
	electrónicos.
Finalidad	Controla que los datos almacenados en la base de datos guarden directa relación con la finalidad legal para la cual se recolectaron.

Tabla 23. Factores que influyen en el derecho de consentimiento

Derecho de Protección de Datos: Consentimiento	
Factores	**Descripción**
Autorización del titular del dato	Verifica que los titulares hayan dado por escrito el consentimiento del tratamiento de sus datos antes de ser recolectados.
Procedimiento de publicación de datos personales	Comprueba que la organización tiene el consentimiento del titular para publicar sus datos en páginas Web.

Tabla 24. Factores que influyen en el derecho de datos sensibles

Derecho de Protección de Datos: Datos sensibles	
Factores	**Descripción**
Autorización para la administración de los datos sensibles	Revisa que la organización tenga un permiso para gestionar datos sensibles, desde la recogida y registro de información hasta su utilización.
Registros de operación de los datos	Verifica la existencia de registros que permitan conocer los procedimientos que se le realizan a los datos sensibles del titular.
Acceso a datos sensibles	Comprueba que la organización en su sistema tenga acceso restringido a los datos sensibles, por lo tanto, solo el personal autorizado puede utilizar y tener acceso a estos.
Publicación de datos sensibles	Control que tiene en cuenta si datos sensibles son publicados en medios de fácil acceso al público (páginas Web, carteleras) y si poseen la autorización para hacerlo.
Soporte informático	Examina que las unidades de almacenamiento (CD, Disco Duro, Memoria USB) que tengan información de datos sensibles solo podrán ser traslada a otro lugar bajo medidas de seguridad y con el permiso del responsable de los datos en la entidad.

Tabla 25. Factores que influyen en el derecho de seguridad de los datos.

Derecho de Protección de Datos: Seguridad de datos	
Factores	**Descripción**
Medidas técnicas de seguridad	Control sobre las medidas necesarias para garantizar la seguridad de los datos en sistemas, centros de cómputos, software y hardware, equipos, personas que utilizan y manejan la información almacenada en las bases de datos.

Derecho de Protección de Datos: Seguridad de datos	
Factores	**Descripción**
Documentación de los sistemas de información	Verifica la existencia de documentación del sistema de información que se utiliza para el tratamiento de datos, con sus respectivas funciones, diagramas, estructura de base de datos, entre otras cosas.
Estructura de las bases de datos	Comprueba que la estructura de la base de datos posea un diseño físico y lógico, e igualmente un diccionario de datos.
Cambios en la estructura de la base de datos	Controla las modificaciones que se realizan a las bases de datos, con requisitos como: autorización para hacerlas, documentación de los respectivos cambios, entre otras cosas.
Registros de incidencias	Verifica el procedimiento de notificación y gestión de cualquier anomalía que afecte la seguridad de los datos, contenidas en un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se pueden derivar de la misma.
Gestión de soporte	Comprueba la existencia de inventarios de los soportes informáticos que almacenan datos personales y registros de autorización para el traslado de estos hacia otras dependencias de la empresa u otras entidades.
Copias de seguridad y recuperación de datos	Copia de seguridad o backup, es una medida de seguridad contra la pérdida de datos en caso de que ocurra una eventualidad, la cual consiste en elaborar una copia de un programa informático, de un disco o de archivo de datos, realizada para archivar su contenido o para proteger archivos valiosos que permiten recuperar y restaurar la base de datos hasta la última unidad de trabajo realizada antes de producirse un error de hardware o de software que haya impedido seguir utilizando la base de datos.
Seguridad física de los equipos	Describe los controles necesarios para mantener con acceso restringido las instalaciones que contienen equipos de cómputos por los cuales se acceden y almacenan datos, asimismo deben utilizarse otros controles físicos(cámaras, sensores, alarmas) que permitan mantener la seguridad en los equipos.
Identificación y autenticación	Procedimiento de reconocimiento y comprobación de la identidad de un usuario. Mediante este factor se garantiza que el usuario que accede a un sistema de información cuente con el permiso del administrador y esté registrado en el sistema.
Control de acceso	Mecanismos que por medio de la identificación y autenticación permite acceder a datos o recursos solo a personal autorizado de acuerdo sus funciones y obligaciones.
Restauración de datos	Verifica que la organización tenga medidas de seguridad para restaurar datos cuando ocurre un error en el sistema, de tal manera que se pueda continuar con el procesamiento de estos.
Funciones y obligaciones del personal	Este factor permite documentar y conocer las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información.

Derecho de Protección de Datos: Seguridad de datos	
Factores	**Descripción**
Pruebas con datos personales	Este factor es para garantizar que durante las pruebas con datos personales, se tomen las medidas necesarias para que los datos se conserven de forma segura. Además debe realizarse una documentación de las pruebas y registrar el personal que tuvo acceso a los datos en caso que estos sean reales.
Planes de contingencia	Herramienta con una serie de procedimientos que permite definir acciones y restituir rápidamente los servicios de una organización ante la eventualidad de que ocurra una falla en los sistemas de información y equipos de cómputo de manera parcial o total.

Tabla 26. Factores que influyen en el derecho del deber de secreto

Derecho de Protección de Datos: Deber de secreto	
Factores	**Descripción**
Compromiso de reserva de información	Verifica que la información personal de una organización no sea revelada sin el consentimiento del afectado.
Autorización limitada a las funciones y actividades a desempeñar	Controla que cada usuario acceda únicamente a los datos y recursos necesarios para el desarrollo de sus funciones

Tabla 27. Factores que influyen en el derecho de comunicación de datos o cesión

Derecho de Protección de Datos: Comunicación de datos o Cesión	
Factores	**Descripción**
Certificado de cesión de datos	Verifica la existencia de documentos que certifiquen la cesión y recepción de datos, en los cuales debe estar claramente definida su finalidad y el consentimiento del titular.
Peticiones de cesión de datos	Examina las peticiones de cesión de datos de parte del titular para su beneficio y aquellas realizadas con fines investigativos y estadísticos.
Control de cesión de datos	Verifica que los datos cedidos cumplan con los requerimientos como: autorización del titular y procedimientos formales para controlarla a través de la red.

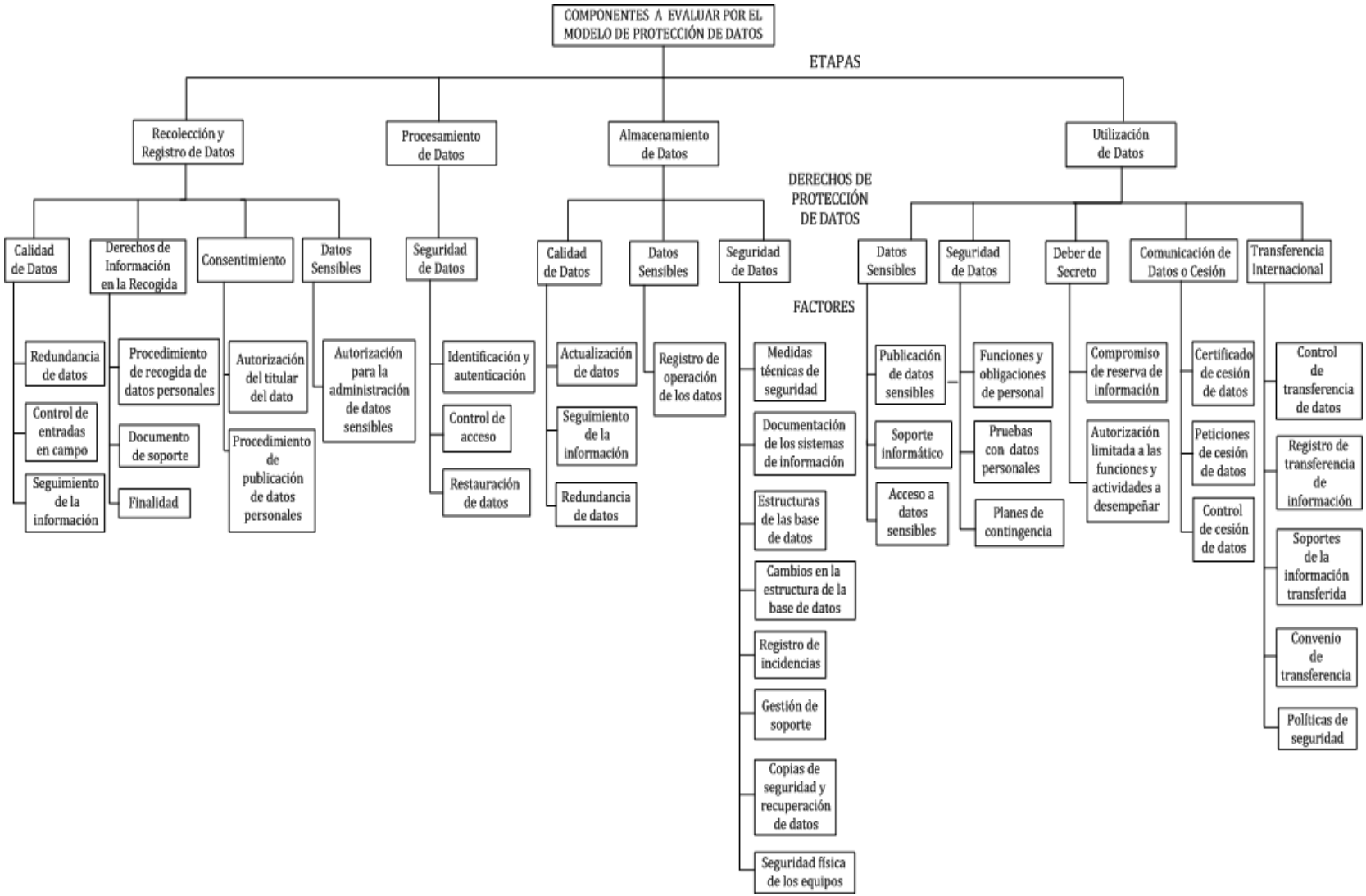
Tabla 28. Factores que influyen en el derecho de transferencia internacional

Derecho de Protección de Datos: Transferencia internacional	
Factores	**Descripción**
Control de transferencia de datos	Comprueba si existen documentos que autoricen las transferencias de datos y si el destinatario garantiza que la información será para fines legales y éticos.
Registro de transferencia	Verifica si la organización posee registros de las transferencias

Derecho de Protección de Datos: Transferencia internacional	
Factores	**Descripción**
de información.	realizadas y si realizan copias de seguridad de cada información transferida.
Soportes de la información transferida.	Controla la transferencia de datos teniendo en cuenta la autorización de la organización y la existencia de soportes de información que verifique el consentimiento del titular.
Convenio de transferencia.	Verifica la existencia de acuerdos con otros países para realizar transferencias de información, en los cuales se define un calendario de envíos y acciones a tomar cuando se sospeche de actividades no autorizadas en dichas transferencias.
Políticas de seguridad.	Comprueba si la organización y el país destinatario tienen documentos que denotan un compromiso con la seguridad de la información y si el titular fue informado de la finalidad del tratamiento de sus datos.

En resumen, para determinar el nivel de cumplimiento de los derechos de protección de datos en un sistema de información, el modelo posee tres componentes a evaluar como son, inicialmente los factores, los cuales pertenecen a los derechos de protección de datos y estos a su vez pertenecen a las etapas del procesamiento de datos; finalmente el estudio de estos componentes permiten la evaluación del sistema de información que sirve de apoyo a los procesos seleccionados. La Figura 8 representa lo planteado anteriormente.

Figura 8. Componentes a evaluar por el modelo de protección de datos.



4.1.3 Indicadores de evaluación

Los indicadores de evaluación que se utilizaron para hallar el cumplimiento de los derechos de protección de datos, se clasifican en los siguientes niveles:

Alto: el derecho de protección de datos se cumple de forma total en un sistema de información.

Medio: el derecho de protección se cumple de manera parcial.

Bajo: el derecho de protección no se cumple.

Teniendo en cuenta que los indicadores para el nivel de cumplimiento de los derechos de protección de datos ya están definidos, se requiere de un criterio para la medición de las variables de análisis, que establece el rango en que se encuentra cada indicador de medición, los cuales se muestran en la Tabla 29.

Tabla 29. Indicadores de evaluación y criterios de medición.

INDICADOR	CRITERIO DE MEDICIÓN
ALTO	De 1.60 a 2.00
MEDIO	De 1.00 a 1.59
BAJO	De 0.00 a 0.99

4.2 SISTEMA DE ACTIVIDAD HUMANA – SAH – PROPUESTO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN

Siguiendo la metodología de sistemas blandos expuesta en el capítulo 2, a continuación se presenta el SAH, que es considerado como el sistema pertinente para desarrollar y aplicar el proyecto planteado, el cual se deriva de los hallazgos y la imagen enriquecida que expresan la situación problema y la definición raíz.

4.2.1 Hallazgos de la situación problema

Al examinar la situación problema se notó que en materia de protección de datos, Colombia aún no cuenta con una ley que controle el manejo de la información, de

igual manera no existen mecanismos técnicos aplicables a los sistemas de información que proporcionen un nivel adecuado y que se garantice el buen manejo de la información.

Sin embargo, el único mecanismo rápido que tiene el titular de la información para solicitar protección en materia de administración de su información es interponer una acción de tutela. Actualmente la Corte Constitucional está estudiando la aprobación de una nueva ley de habeas data que no regula todos los parámetros necesarios e impuestos en los tratados Internacionales; la cual no es impedimento para que los administradores de bases de datos no apliquen herramientas técnicas necesarias para actualizar, verificar, eliminar, conocer, rectificar y proteger la información personal en los sistemas de información.

En la investigación realizada se han identificado algunos problemas que se presentan en los sistemas de información con la administración de los datos, que permiten registrase como hallazgos de la situación problema:

- Inconformidad por parte del titular de la información de la manera como son administrados sus datos.
- No toda la información que se encuentra en las bases de datos es veraz, correcta y actualizada.
- No existe una cultura de protección de datos personales por parte de los administradores de la base de datos.
- Incorporación de información errónea en los sistemas de información.
- Los administradores de información transmiten la información a otras entidades o terceros.
- Los datos son manipulados, distribuidos y comercializados sin el consentimiento del titular de la información.
- No existen sanciones legales para el uso inadecuado de los datos personales recolectados en bancos de datos.

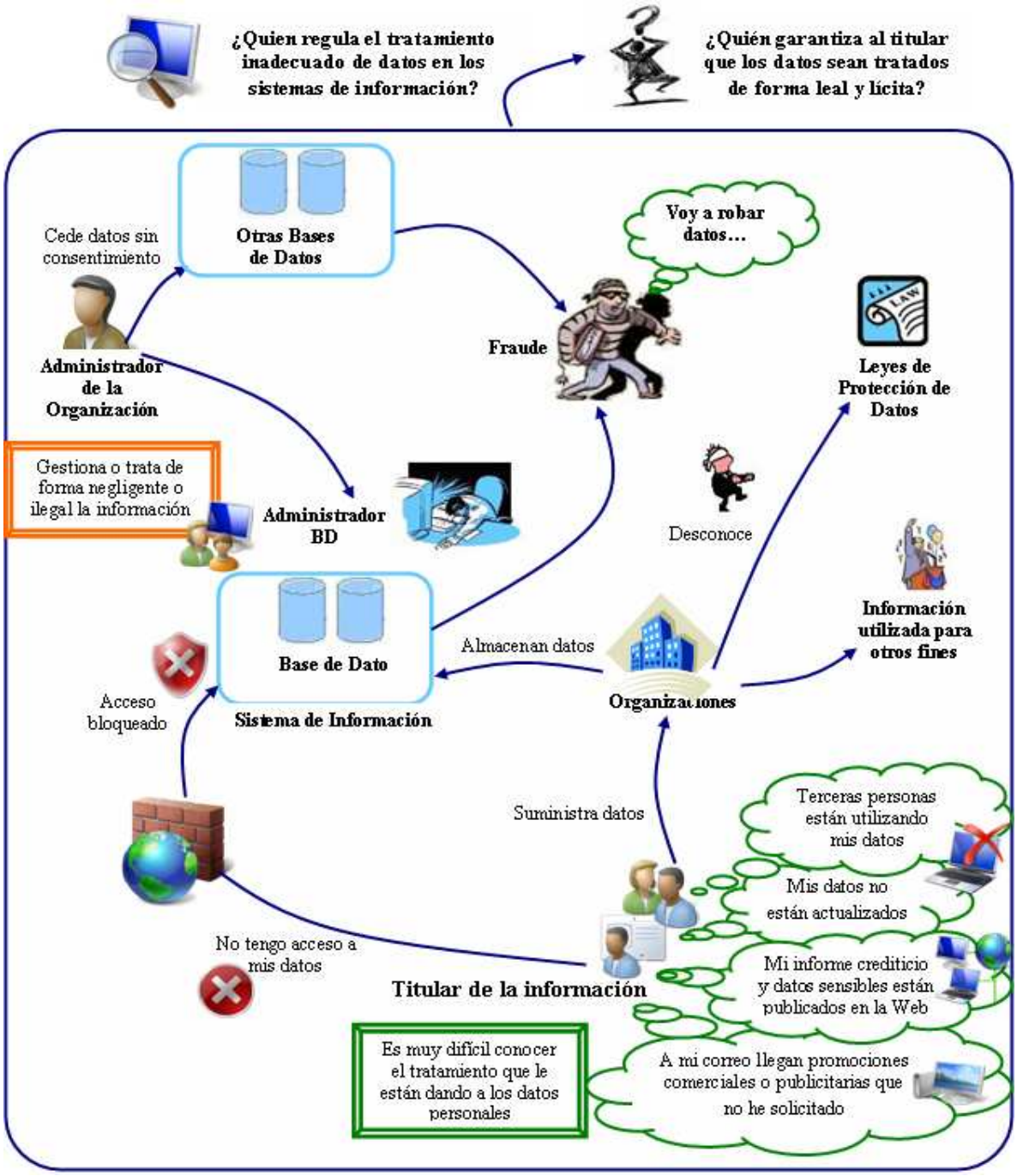
- Ausencia de un ente de control que vigile a los administradores de los bancos de datos, en cuanto al uso inadecuado de los datos.
- No hay quien garantice la seguridad de la información de manera que no sea accedida por personas no autorizadas.

A continuación en la Figura 9, se muestra una imagen que ilustra los hallazgos anteriormente descritos, la cual contribuye a una mayor comprensión del problema y del contexto de la situación de interés.

4.2.2 Imagen enriquecida de la situación real

La Figura 9 representa la situación problema sobre la protección de datos personales. En ella se puede observar que el titular de los datos expresa los inconvenientes presentados en el manejo de su información, por parte de las organizaciones a los que ellos ceden o suministran sus datos personales, que almacenan en las bases de datos de sus sistemas de información, pero en algunos casos estos no tienen acceso a sus datos almacenados en los sistemas de la organización. Por otra parte, administradores de la organización autorizan ceder datos de los titulares a otras bases de datos fuera de la organización sin su consentimiento, igualmente algunos administradores de bases de datos gestionan de forma negligente o ilegal la información, lo cual con lleva que esta sea de fácil acceso por personas ajenas a la organización, contribuyendo al fraude y al robo de información. Ciertas organizaciones utilizan la información almacenada en sus bases de datos para fines distintos para los cuales estos fueron recolectados, tales como envíos de avisos publicitarios, lanzamientos de nuevos productos, invitaciones a campañas políticas. Una de las razones por las que organizaciones realizan las acciones anteriormente mencionadas, es el desconocimiento de las leyes de protección de datos. Ante todo esto surgen dos grandes inquietudes ¿Quién regula el tratamiento inadecuado de datos en los sistemas de información? y ¿Quién garantiza al titular que los datos sean tratados de forma leal y lícita?

Figura 9. Imagen enriquecida de la situación de interés.



4.2.3 Definición raíz – DR

Después de ilustrar la situación de interés se procede a nombrar los sistemas pertinentes a través de la DR, que describe un conjunto de actividades con

propósito definido, la cual realiza un proceso de transformación deseable para la situación problema (Ver Tabla 30).

Tabla 30. Definición raíz de la situación de interés del trabajo de investigación

DEFINICION RAÍZ
Un sistema propiedad de los autores, programa de Ingeniería de Sistemas de la Universidad del Magdalena y el grupo STI, que permitan a las organizaciones que manejen datos de carácter personal, evaluar el cumplimiento de los derechos de protección de datos en los sistemas de información con apoyo de tecnología de información, teniendo como lineamiento las leyes de protección de datos a nivel nacional e internacional, con el fin de evitar la violación del derecho del habeas data y mejorar el buen uso y administración de la información.

Para detallar la DR, se requiere de la utilización del mnemónico CATWOE de la situación problema, que se describe en la Tabla 31.

Tabla 31. Elementos del CATWOE de la situación problema

Elementos del CATWOE		
Sigla	**Elemento**	**Descripción**
C	**Cliente**	· Organizaciones que administran datos de carácter personal por medio de un sistema de información. · Titular de los datos.
A	**Actores**	Equipo desarrollador del proyecto: · Autores de proyecto. · Grupo de Investigación en Sistemas y Tecnología de la Información – STI.
T	**Transformación**	Necesidad de proteger y mejorar el uso y administración de los datos de carácter personal y hacer cumplir el derecho del habeas data en los sistemas de información. → Necesidad satisfecha.
W	**Weltanschaung**	Buscar mecanismos que permitan evaluar el cumplimiento de los derechos de protección de datos en un sistema de información, y dar sugerencias para evitar la violación del derecho de habeas data y mejorar el buen uso y administración de la información.
O	**Propietarios**	· Autores del proyecto. · Programa de Ingeniería de Sistemas de la Universidad del Magdalena. · Grupo de Investigación en Sistemas y Tecnología de la Información – STI.
E	**Restricciones**	· Los derechos de protección de datos definidos según el estudio de las leyes a nivel nacional e internacional. · La organización que ejecute el proyecto aplique las

Elementos del CATWOE		
Sigla	**Elemento**	**Descripción**
		recomendaciones dadas por el diagnóstico del modelo.

4.3 MODELO DE ACTIVIDADES PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN

Continuando con la metodología de sistemas blandos y teniendo la definición raíz construida, se definió un modelo de actividades que presenta los pasos a seguir para estudiar y evaluar el cumplimiento de los derechos de protección de datos en los diferentes procesos de una organización que utilizan datos personales y son administrados por una herramienta tecnológica.

Una de las actividades comprende, proporcionar al evaluador una guía que incorpora los mecanismos de recolección de información definidos para su utilización en la aplicación del modelo, y formatos para analizar la información recopilada teniendo en cuenta el estudio de las leyes de protección de datos realizado en el capítulo 3 y los indicadores de evaluación establecidos; de igual forma se establecen formatos para presentar los resultados de la aplicación y las recomendaciones que deben ser sugeridas de acuerdo a la evaluación obtenida, para lograr la transformación esperada y poder garantizar el derecho de habeas data al titular de la información. Todo lo anterior es lo establecido en el segundo objetivo de la propuesta de investigación[58].

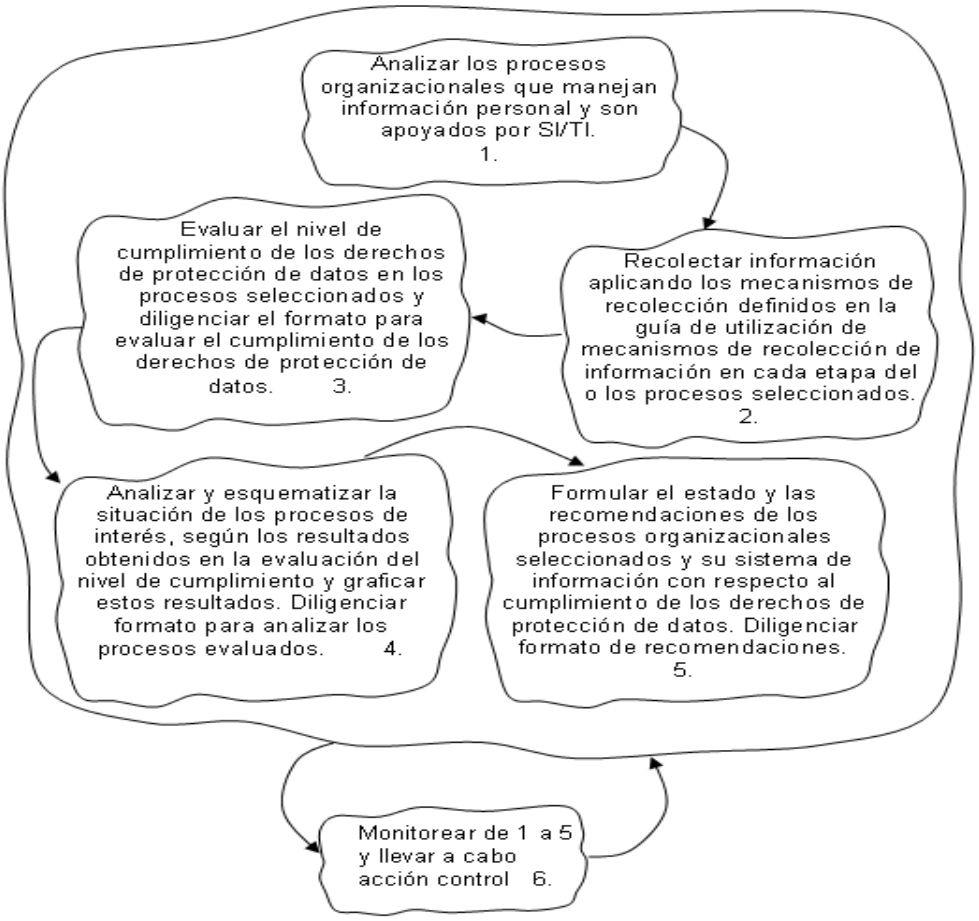
La Figura 10 muestra el modelo general con el conjunto de actividades necesarias para evaluar el nivel de cumplimiento de los derechos de protección de datos en

[58] El segundo objetivo determina lo siguiente:

- Construir un modelo basado en el estudio realizado que contenga las siguientes funciones:
  - Definir los mecanismos de recolección de información, tales como: encuestas, formularios, cuestionario de entrevistas, observaciones directas del sistema, etc.
  - Analizar la información recopilada por el modelo, teniendo en cuenta las leyes de la protección de datos y los indicadores de evaluación, para verificar el cumplimiento de estos en un sistema de información.
  - Presentar los resultados obtenidos de la aplicación mediante los indicadores de evaluación.

los procesos de una organización que utiliza datos personales y son apoyados por una herramienta tecnológica.

Figura 10. Modelo de Sistema de Actividades Humanas para la definición raíz.



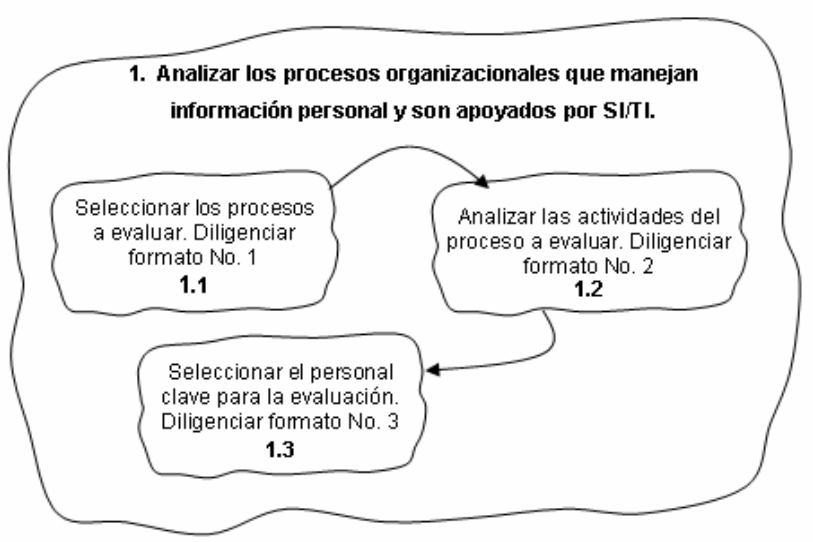
El modelo de sistemas de actividades humanas propuesto debe tener en cuenta que para la aplicación del modelo es necesario, analizar los procesos organizacionales que manejan información personal y son apoyados por una herramienta tecnológica, recolectar la información con el apoyo de la guía de utilización de los mecanismos de recolección de información, para luego evaluar el nivel de cumplimiento de los derechos de protección de datos, analizar y esquematizar la situación de los procesos de interés, y según los resultados obtenidos en la evaluación, se podrá formular el estado y las recomendaciones para los procesos organizacionales que son apoyados por los sistemas de

información evaluados; sobre todas esta actividades se debe monitorear y llevar a cabo acción de control. A continuación se presenta una descripción detallada de cada una de las actividades del modelo de SAH:

4.3.1 Actividad 1. Analizar los procesos organizacionales que manejan información personal y son apoyados por SI/TI

En esta actividad se realiza el primer contacto con la organización, inicialmente es necesario que el evaluador realice un estudio preliminar a los procesos que se llevan a cabo en las áreas o dependencias de la organización, el cual se debe centrar en los que son apoyados por tecnologías de información y administran datos personales; este estudio comprende tres actividades básicas, las cuales se muestran en la Figura 11.

Figura 11. SAH de la actividad 1



En la Tabla 32 se presenta la descripción del SAH de la actividad 1.

Tabla 32. Descripción del SAH de la actividad 1.

Act.	Nombre Actividad	Descripción
A1.1	Seleccionar los proceso a evaluar	Para aplicar el modelo, el evaluador debe explorar los procesos realizados en la organización, teniendo en cuenta que estos deben manejar información personal y ser apoyados por SI/TI, para determinar el o los procesos a evaluar. Para ello se utiliza el formato Nº 1.Selección de los procesos a evaluar (Ver figura 12); en donde el evaluador indica cual de los procesos estudiados es el seleccionado a evaluar.
A1.2	Analizar las actividades de los procesos a evaluar	En esta actividad, el evaluador debe consultar las actividades realizadas en los procesos seleccionados a evaluar, con el fin de comprender el funcionamiento de estos, identificar el personal que interviene en cada una de las etapas del procesamiento de datos y recolectar una información adecuada para optimizar los resultados de la auditoria de protección de datos a realizar; para llevar a cabo esta actividad el evaluador cuenta con el apoyo del formato Nº 2. Análisis de las actividades del proceso a evaluar (Ver figura 13).
A1.3	Seleccionar el personal clave para la evaluación	Después de analizar y seleccionar los procesos organizacionales a evaluar y describir sus actividades; en esta actividad se selecciona el personal clave para la evaluación, para esto se debe tener en cuenta a los administradores de TI y a las personas que intervienen en las etapas del procesamiento de los datos; el evaluador debe identificar y seleccionar según su criterio el personal más conveniente para realizar la evaluación de acuerdo al estudio realizado a la organización (Ver figura 14, forma Nº 3).

Figura 12. Formato Nº 1. Selección de procesos a evaluar.

***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO N° 1. SELECCIÓN DE PROCESOS A EVALUAR

Este formato permite seleccionar los procesos organizacionales que serán evaluados para determinar el nivel de cumplimiento de los derechos de protección de datos.

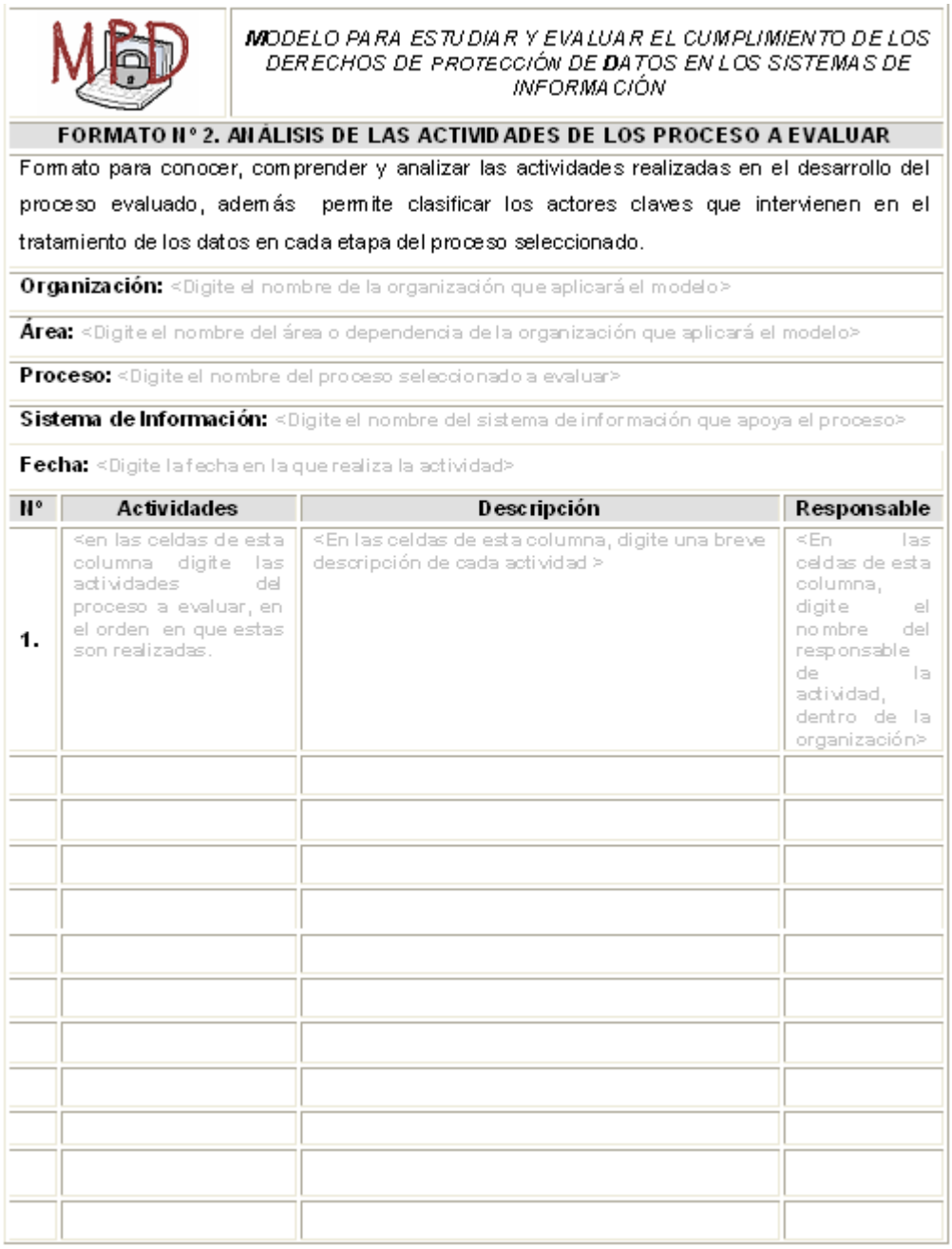
Organización: <digite el nombre de la organización que aplicará el modelo>

Área: Digite el nombre del área o dependencia de la organización que aplicara el modelo>

Responsable: <digite el responsable o director del área>

Proceso	Manejo información personal	Apoyo SI/TI	Proceso seleccionado
<En estas celdas digite los nombres de los procesos que maneja la dependencia que aplicara el modelo>	<Digite una 'X' si los procesos manejan información personal>	<Digite una 'X' si los procesos tienen apoyo de SI/TI>	<Digite una 'X' si los procesos manejan información personal y tienen apoyo SI/TI>

Figura 13. Formato Nº 2. Análisis de las actividades de los procesos a evaluar.



MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN

FORMATO N° 2. ANÁLISIS DE LAS ACTIVIDADES DE LOS PROCESO A EVALUAR

Formato para conocer, comprender y analizar las actividades realizadas en el desarrollo del proceso evaluado, además permite clasificar los actores claves que intervienen en el tratamiento de los datos en cada etapa del proceso seleccionado.

Organización: <Digite el nombre de la organización que aplicará el modelo>

Área: <Digite el nombre del área o dependencia de la organización que aplicará el modelo>

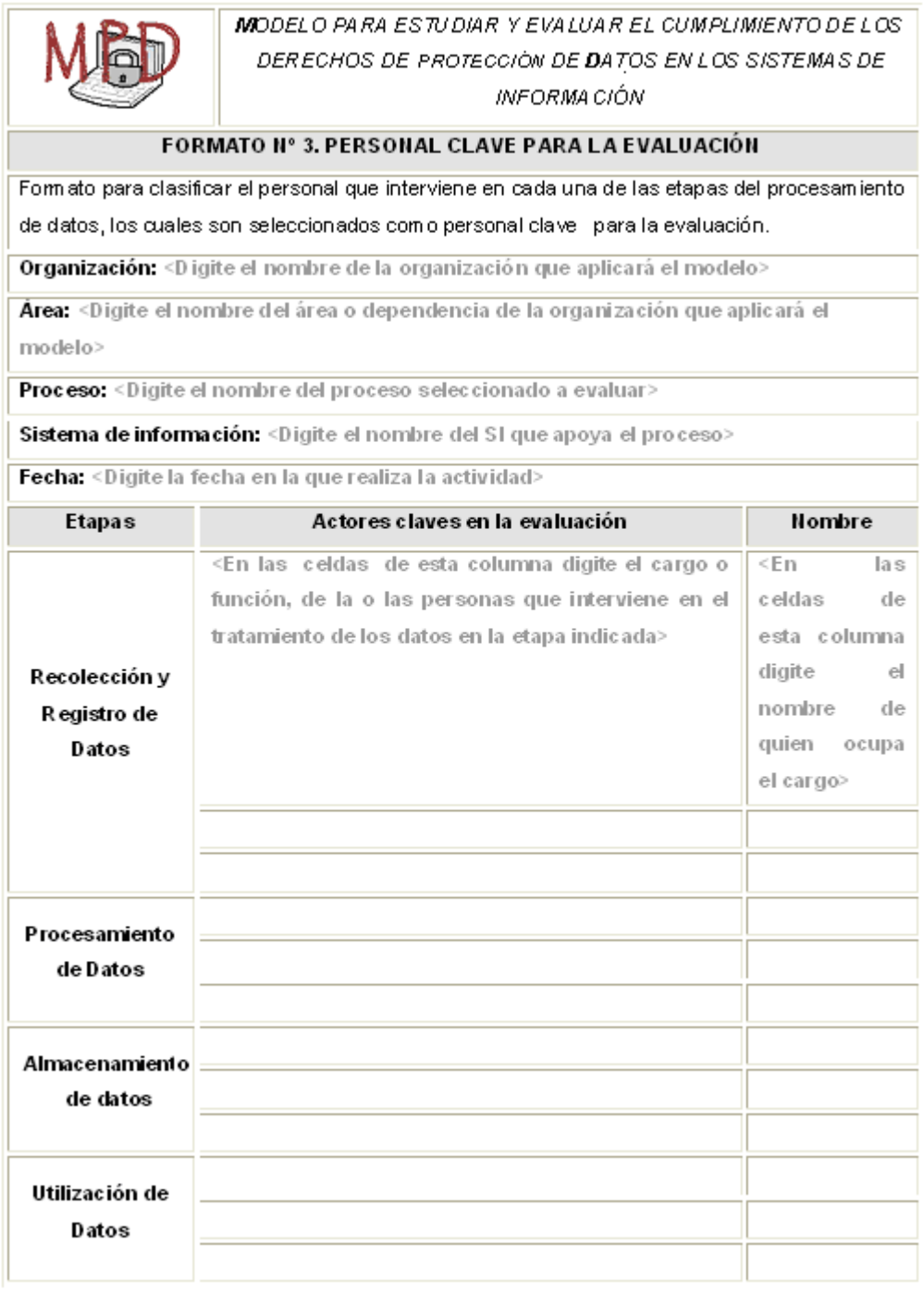
Proceso: <Digite el nombre del proceso seleccionado a evaluar>

Sistema de Información: <Digite el nombre del sistema de información que apoya el proceso>

Fecha: <Digite la fecha en la que realiza la actividad>

N°	Actividades	Descripción	Responsable
1.	<en las celdas de esta columna digite las actividades del proceso a evaluar, en el orden en que estas son realizadas.	<En las celdas de esta columna, digite una breve descripción de cada actividad >	<En las celdas de esta columna, digite el nombre del responsable de la actividad, dentro de la organización>

Figura 14. Formato Nº 3. Personal clave para la evaluación.



MPD	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO N° 3. PERSONAL CLAVE PARA LA EVALUACIÓN

Formato para clasificar el personal que interviene en cada una de las etapas del procesamiento de datos, los cuales son seleccionados como personal clave para la evaluación.

Organización: <Digite el nombre de la organización que aplicará el modelo>

Área: <Digite el nombre del área o dependencia de la organización que aplicará el modelo>

Proceso: <Digite el nombre del proceso seleccionado a evaluar>

Sistema de información: <Digite el nombre del SI que apoya el proceso>

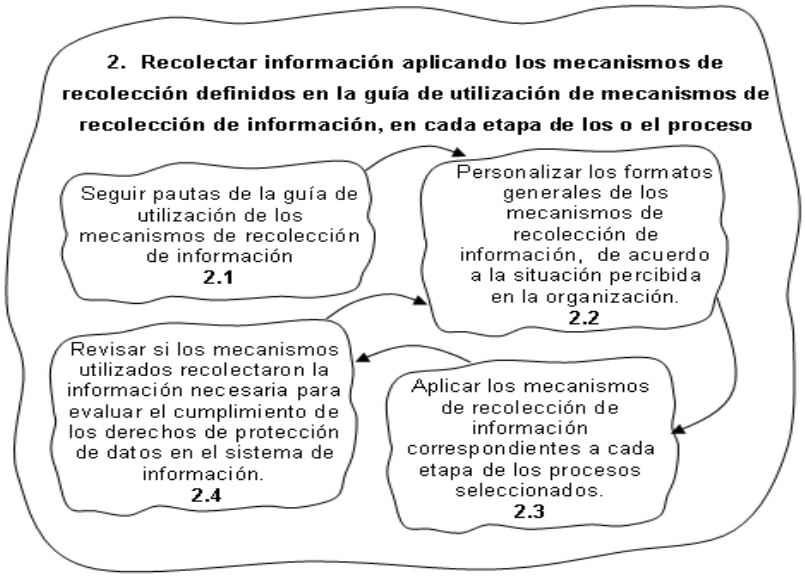
Fecha: <Digite la fecha en la que realiza la actividad>

Etapas	Actores claves en la evaluación	Nombre
Recolección y Registro de Datos	<En las celdas de esta columna digite el cargo o función, de la o las personas que interviene en el tratamiento de los datos en la etapa indicada>	<En las celdas de esta columna digite el nombre de quien ocupa el cargo>
Procesamiento de Datos		
Almacenamiento de datos		
Utilización de Datos		

4.3.2 Actividad 2. Recolectar información aplicando los mecanismos de recolección definidos en la guía de utilización de mecanismos de recolección de información, en cada etapa de los procesos seleccionados

Esta actividad es muy importante, ya que las demás actividades dependen de esta, por lo tanto, se debe recolectar la información necesaria para determinar el nivel de cumplimiento de los derechos de protección de datos que realmente tienen los sistemas de información que utiliza la organización a estudiar. Para facilitar esta actividad y recolectar la información necesaria y adecuada, los diseñadores del presente modelo, proporcionan una guía al evaluador (Ver tablas 34 - 46) que indican los mecanismos para recolectar la información necesaria para la evaluación, llamada guía de utilización de los mecanismos de recolección de información la cual debe ser personalizada según las actividades realizadas en la organización. De igual forma, el modelo de SAH propuesto permite al evaluador revisar si los mecanismos utilizados recolectaron la información necesaria para el estudio, de lo contrario se requiere una nueva recolección de información. En la Figura 15 se muestra el sistema de actividad humana para la actividad 2.

Figura 15. SAH de la actividad 2.



La Tabla 33 presenta la descripción de cada una de las actividades que comprende la actividad 2.

Tabla 33. Descripción de SAH de la actividad 2.

Act.	Nombre Actividad	Descripción
A2.1	Seguir pautas de la guía de utilización de los mecanismos de recolección de información	El evaluador debe consultar la guía de utilización de los mecanismos de recolección de información. (Ver tablas 34 - 46)
A2.2	Personalizar los formatos generales de los mecanismos de recolección de información, de acuerdo a la situación percibida en la organización.	De acuerdo al análisis realizado a los procesos en la actividad 1, y la consulta realizada a la guía en la actividad A2.1, el evaluador debe establecer que derechos de protección de datos o factores son aplicables en la organización para realizar la correcta evaluación a los procesos. De esta forma los formatos generales de mecanismos de recolección de información propuestos por los diseñadores, quedan personalizados de acuerdo a las actividades realizadas en la organización; es decir, si un factor o derecho de protección de datos no es aplicable a la organización o proceso de interés se debe descartar su evaluación.
A2.3	Aplicar los mecanismos de recolección de información correspondientes a cada etapa de los procesos seleccionados.	En esta actividad se recolecta la información al personal clasificado por cada etapa, para estudiar cada una de los derechos de protección de datos en los procesos seleccionados; todo lo anterior se lleva a cabo a través de los formatos personalizados en la actividad anterior (A2.2).
A2.4	Revisar si los mecanismos utilizados recolectaron la información necesaria para evaluar el cumplimiento de los derechos de protección de datos en el sistema de información	En esta etapa se verifica si la información recolectada es suficiente para evaluar el cumplimiento de los derechos de protección de datos en el sistema de información, de lo contrario se requiere aplicar nuevamente los mecanismos de recolección a otros funcionarios de la organización o recolectar información con otros mecanismos dentro de los propuestos.

A continuación se presenta el esquema general de la guía de utilización de los mecanismos de recolección de información, dividida en las cuatro etapas de procesamiento de datos definidas y a su vez esta se divide en cada derecho de protección de datos a evaluar.

4.3.2.1 Guía 1. Utilización de los mecanismos de recolección de información para la etapa de recolección y registro de datos - derecho de protección de datos: calidad de datos

Tabla 34. Descripción de la Guía 1.

Etapa de Recolección y Registro de Datos		
Derecho de Protección de Datos: Calidad de Datos		
Factor	**Interrogante**	**Mecanismo**
Redundancia de Datos	1. Al recolectar datos, ¿se verifica que en las diferentes áreas de la organización no estén recolectando de manera independiente la misma información?	Entrevista
	2. ¿Los datos personales recolectados y registrados en el sistema de información son almacenados en una misma base de datos para toda la organización?	
Control de Entradas en Campos	3. ¿El ingreso de datos a los campos de la base de datos se realiza con previa autorización?	Entrevista y observación
	4. Al registrar datos en los sistemas de información, ¿verifica que los datos ingresados correspondan con el campo indicado en la base de datos?	
	5. ¿Se lleva acabo un control detallado de los datos que se registran en los campos de la base de datos?	
	6. ¿Al registrar los datos en el sistema de información, poseen controles para que en cada campo se digite el formato (número o letra) y el tamaño adecuado?	Consulta al sistema
	7. ¿Al registrar datos, se tiene control sobre la entrada de los campos obligatorios, para que no sean llenados en blanco?	
	8. ¿Se tiene un rango máximo y mínimo al número de caracteres o dígitos a digitar en cada campo?	
	9. ¿En el sistema se realiza una prenumeración de formatos para el ingreso de datos o registros de transacciones? ¿El sistema controla la secuencia de los formatos prenumerados?	
Seguimiento de la Información	10. ¿Se definen los medios para recolectar la información antes de que los datos sean almacenados en una base de datos, de manera que estos no sean recolectados por medios desleales o fraudulentos?	Entrevista y revisión de documentos
	11. Al recolectar y registrar datos personales en los sistemas de información, ¿se asegura que sean reales, completos y actualizados?	Entrevista y revisión de documentos

4.3.2.2 Guía 2. Utilización de los mecanismos de recolección de información para la etapa de recolección y registro de datos - derecho de protección de datos: información en la recogida de datos

Tabla 35. Descripción de la Guía 2.

Etapa de Recolección y Registro de Datos		
Derecho de Protección de Datos: Información en la Recogida de Datos		
Factor	**Interrogante**	**Mecanismo**
Procedimiento de Recogida de Datos Personales	1. ¿Al titular de los datos se le ha informado de forma expresa, precisa y clara de los siguientes aspectos?	Entrevistas y Encuestas
	1.1 De la creación de una base de datos propiedad de la entidad donde serán almacenados sus datos personales.	
	1.2 Del propósito de la recogida de los datos, la finalidad para la que serán tratados y quienes pueden ser los destinatarios de la información.	
	1.3 Del carácter obligatorio o facultativo de suministrar los datos que le sean solicitados, y las consecuencias de proporcionar datos no exactos o falsos al momento de recolectar la información.	
	1.4 De la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición de los datos que serán almacenados en bases de datos.	
	2. ¿Su entidad recolecta los datos directamente del titular de la información?	Entrevista
	3. Si la anterior respuesta es negativa, ¿dispone de algún método para informarle de este hecho y de la fuente de la que provienen los datos?	Entrevista y revisión de documentos
Documento de Soporte	4. Al momento de recolectar y registrar datos personales en bases de datos, ¿solicita una autorización por escrito o posee formatos firmados por el titular, en donde se evidencie que proporciona sus datos personales de manera voluntaria?	Entrevista y revisión de documentos
	5. Si su organización utiliza documentos, cuestionarios, formularios impresos o electrónicos u otros mecanismos de recogida y registro de datos online ¿incluyen en estos, información sobre el tratamiento y la finalidad de la recogida de estos datos y los posibles destinatarios de la información?	
	6. ¿De los documentos recolectados existe en el sistema de información un registro de estos?	Entrevista y revisión de documentos o consultas al sistema

Etapa de Recolección y Registro de Datos		
Derecho de Protección de Datos: Información en la Recogida de Datos		
Factor	**Interrogante**	**Mecanismo**
Finalidad	7. ¿Los datos de carácter personal almacenados en la base de datos guardan directa relación con la finalidad legal para la cual se recolectan?	Entrevista y consultas al sistema

4.3.2.3 Guía 3. Utilización de los mecanismos de recolección de información para la etapa de recolección y registro de datos - derecho de protección de datos: consentimiento

Tabla 36. Descripción de la Guía 3.

Etapa de Recolección y Registro de Datos		
Derecho de Protección de Datos: Consentimiento		
Factor	**Interrogante**	**Mecanismo**
Autorización del Titular del Dato	1. Al recolectar y registrar datos personales en bases de datos, ¿Su entidad solicita el consentimiento expreso y por escrito al titular para tratar estos datos, ya sea un documento o formularios empleados en la recogida de datos con cláusulas de consentimiento y firmados por el titular?	Entrevista y revisión de documentos
Procedimiento de publicación de datos personales	2. En el momento de registrar datos, ¿el área o dependencia solicita el consentimiento del titular de la información para publicar sus datos en páginas Web?	Entrevista y revisión de documentos
	3. Si su entidad recolecta datos online, ¿posee formularios con cláusulas o políticas de seguridad, en donde le indique al titular que debe dar el consentimiento para que sus datos puedan ser almacenados y tratados en una base de datos propiedad de la organización?	

4.3.2.4 Guía 4. Utilización de los mecanismos de recolección de información para la etapa de recolección y registro de datos - derecho de protección de datos: datos sensibles

Tabla 37. Descripción de la Guía 4.

Etapa de Recolección y Registro de Datos		
Derecho de Protección de Datos: Datos Sensibles		
Factor	**Interrogante**	**Mecanismo**
Autorización para la Administración de Datos Sensibles	Si su organización recolecta y registra en sus bases de datos, datos sensibles, como son los referentes a origen racial y étnico, ideología, afiliación sindical, religión, opiniones políticas, creencias, salud, o vida sexual	
	1. Al recolectar datos sensibles ¿Se solicita el consentimiento previo por escrito del titular para registrar y tratar estos datos en sistemas de información de su organización?	Entrevista y revisión de documentos
	2. Antes de registrar datos personales en bases de datos, ¿se le informa al titular de los datos del derecho a no declarar sobre su ideología, religión o creencias?	Entrevista

4.3.2.5 Guía 5. Utilización de los mecanismos de recolección de información para la etapa de procesamiento de datos - derecho de protección de datos: seguridad de datos

Tabla 38. Descripción de la Guía 5.

Etapa de Procesamiento de Datos		
Derecho de Protección de Datos: Seguridad de Datos		
Factor	**Interrogante**	**Mecanismo**
Identificación y Autenticación	1. ¿La base de datos donde se almacenan los datos personales está protegida por contraseña?	Consultas al sistema
	2. ¿El administrador de la base de datos y los usuarios tienen contraseñas para acceder al sistema de información?	
	3. Si el administrador del sistema crea cuentas a los usuarios, ¿estos se encargan de generar sus contraseñas?	Entrevista
	4. ¿Los usuarios y el administrador de la base de datos cambian periódicamente las contraseñas o claves de acceso a los sistemas?	

Etapa de Procesamiento de Datos		
Derecho de Protección de Datos: Seguridad de Datos		
Factor	**Interrogante**	**Mecanismo**
	5. ¿Las contraseñas utilizadas para acceder a los sistemas tienen definida una longitud mínima y contiene requisitos de complejidad, tales como números o letras?	
	6. ¿Al establecer las contraseñas, los usuarios pueden repetir las últimas contraseñas utilizadas?	
	7. ¿Poseen las contraseñas un tiempo máximo de vigencia, y es obligatorio que se cambien las contraseñas de acceso a los sistemas después de pasado este periodo de vigencia?	
	8. ¿Existen procedimientos de bloqueo y desbloqueos de cuenta por utilización reiterada de contraseñas incorrectas?	Consulta al sistema
	9. ¿Se registran los nombres de usuarios y contraseñas de los accesos no autorizados o rechazados a las estructuras, tablas lógicas y tablas físicas de la base de datos?	Consultas al sistema
	10. ¿Las contraseñas de acceso son almacenadas de forma no legible?	Consultas al sistema
Control de Acceso	11. ¿En la empresa o dependencia existe un administrador de sistemas que gestiona y controla los perfiles de usuarios?	Entrevista
	12. ¿Se controla el acceso de los usuarios a los datos y recursos como sistemas, equipos, programas, aplicaciones, bases de datos, redes, etc, de acuerdo a sus funciones laborales?	Entrevista, consultas al sistema u observación
	13. ¿En los sistemas se puede identificar y auditar los accesos y acciones realizados por cada usuario?	Entrevista y consultas al sistema
	14. ¿Se tiene una lista o tabla actualizada en la base de datos de los usuarios que acceden a los sistemas de información, así como de los usuarios autorizados a acceder y procesar datos en cada uno de los módulos del sistema y sus bases de datos?	
	15. ¿Para los accesos a través de redes de telecomunicaciones, se adoptan las mismas medidas que para los accesos locales?	
Restauración de Datos	16. Al procesar datos personales, ¿existen mecanismos que al reiniciar la ejecución de un proceso interrumpido permitan continuar con el procesamiento de los datos sin repetir o sin dejar de procesar algunas operaciones?	Entrevista, observación

Etapa de Procesamiento de Datos		
Derecho de Protección de Datos: Seguridad de Datos		
Factor	**Interrogante**	**Mecanismo**
	17. Si la anterior respuesta es positiva, al procesar datos personales, ¿los procedimientos establecidos para la recuperación y restauración de datos garantizan la reconstrucción de estos en el estado en el que se encontraban al tiempo de producirse un fallo en el sistema?	

4.3.2.6 Guía 6. Utilización de los mecanismos de recolección de información para la etapa de almacenamiento de datos - derecho de protección de datos: calidad de datos

Tabla 39. Descripción de la Guía 6.

Etapa de Almacenamiento de Datos		
Derecho de Protección de Datos: Calidad de Datos		
Factor	**Interrogante**	**Mecanismo**
Actualización de Datos	1. ¿Se le ha presentado algún evento en el que maneje datos personales de manera inexacta, incompleta o errada?	Entrevista
	2. Para los datos almacenados en bases de datos, ¿posee mecanismos técnicos que conserven los datos de carácter personal exactos y actualizados?	Entrevista y observación o consultas al sistema
	3. ¿Existe un control de los datos personales actualizados en la base de datos?	Entrevista y observación
	4. ¿Se tiene presente que cualquier cambio que se ejecute en los datos personales requiere que se realice en todos los programas o sistemas de la organización que utilizan estos datos?	
Seguimiento de la Información	5. ¿Se realiza algún tipo de seguimiento a la información almacenada en la bases de datos antes de su utilización?	Entrevista y observación
	6. De los datos personales almacenados en las bases de datos, ¿se lleva un seguimiento que pueda verificar que ésta no sea utilizada para finalidades distintas a las determinadas en la recolección?	Entrevista y observación o consultas al sistemas
Redundancia de Datos	7. ¿Se presenta con frecuencia datos duplicados en el sistema de información?	Entrevista y encuesta
	8. ¿Se cancelan inmediatamente datos duplicados en el sistema?	Entrevista
	9. Antes de eliminar datos duplicados se verifica si existe realmente una copia de estos.	

Etapa de Almacenamiento de Datos		
Derecho de Protección de Datos: Calidad de Datos		
Factor	**Interrogante**	**Mecanismo**
	10. ¿Es necesaria una autorización para el administrador de la base de datos en caso que desee eliminar un dato duplicado?	

4.3.2.7 Guía 7. Utilización de los mecanismos de recolección de información para la etapa de almacenamiento de datos - derecho de protección de datos: datos sensibles

Tabla 40. Descripción de la Guía 7.

Etapa de Almacenamiento de Datos		
Derecho de Protección de Datos: Datos Sensibles		
Factor	**Interrogante**	**Mecanismo**
Registro de Operaciones de los Datos	1. De los datos sensibles que son almacenados en el sistema de información, ¿se dispone de un registro de operación que permita conocer los procedimientos que se le realizan a los datos?	Consultas al sistema

4.3.2.8 Guía 8. Utilización de los mecanismos de recolección de información para la etapa de almacenamiento de datos - derecho de protección de datos: seguridad de datos

Tabla 41. Descripción de la Guía 8.

Etapa de Almacenamiento de Datos		
Derecho de Protección de Datos: Seguridad de Datos		
Factor	**Interrogante**	**Mecanismo**
Medidas Técnicas de Seguridad	1. ¿En su organización el administrador de la base de datos ha establecido medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos en sistemas, centros de cómputos, software y hardware, equipos, personas que utilizan y manejan la información almacenada en las bases de datos?	Entrevista
	2. En caso que su organización cuente con estas medidas de seguridad, ¿estas han sido redactadas y documentadas en un documento como políticas o medidas de seguridad para los datos?	Revisión de documentos

Etapa de Almacenamiento de Datos		
Derecho de Protección de Datos: Seguridad de Datos		
Factor	**Interrogante**	**Mecanismo**
	3. ¿En este documento están claramente definidos todas las normas, procedimientos, reglas y estándares, para garantizar un nivel de seguridad que permita la conservación de los datos?	
Documentación de los Sistemas de Información	4. ¿Los sistemas de información utilizados para el manejo de datos personales se encuentran debidamente documentados?	Revisión de documentos
	5. ¿En la documentación se especifica el nombre del sistema que se utiliza para el tratamiento de los datos, sus funciones y otros datos referentes como al equipo servidor en el que se encuentra almacenada la base de datos?	
	6. ¿La documentación del sistema cuenta con los respectivos diagramas y modelos que se utilizaron para el diseño, estructura de la base de datos, diccionario de datos y la descripción de cada una de las entidades que componen las bases de datos?	
Estructura de las Bases de Datos	7. ¿La base de datos dispone de un diseño físico y lógico?	
	8. ¿Posee el diccionario de datos un diseño físico y lógico?	
Cambios en la Estructura de la Base de Datos	9. ¿Es necesaria la autorización del administrador de la base de datos para realizar cambios a la base de datos?	Entrevista
	10. ¿Las modificaciones se realizan sobre una copia de la base de datos?	
	11. ¿Se realiza un bloqueo sobre la parte de la base de datos a modificar?	Entrevista
	12. ¿Se comunica a los diferentes usuarios o desarrolladores del sistema el bloqueo realizado y los posibles fallos de funcionamiento que se pueden presentar?	Encuesta
	13. ¿Se realizan pruebas sobre el cambio realizado para verificar que el sistema funciona correctamente?	Entrevista
	14. ¿Existen registros o bitácoras en donde se documentan y almacenan todos los cambios realizados a la base de datos, como la petición de cambio, script del cambio realizado, entre otros?	Entrevista y revisión de documentos
	15. ¿Se actualiza el diccionario de datos después del cambio realizado en la base de datos?	Revisión de documentos y consultas al sistema
Registro de Incidencias	16. ¿Existe un procedimiento de notificación y gestión de incidencias para la dependencia?	Entrevista y revisión de

Etapa de Almacenamiento de Datos		
Derecho de Protección de Datos: Seguridad de Datos		
Factor	**Interrogante**	**Mecanismo**
	17. Si la anterior respuesta es positiva, ¿se registra el tipo de incidencia, el momento en que se ha producido, persona que realiza la notificación, persona a quien se le comunica y los efectos que se hubieran derivado de la incidencia, además de las medidas adoptadas para la solución?	documento
	18. En caso de que exista este registro de incidencia, ¿este contiene el procedimiento de restauración de datos utilizados, los datos restaurados y datos que fueron restaurados manualmente?	
Gestión de Soporte	19. ¿Poseen inventariado y almacenado todos los soportes informáticos que contienen datos de carácter personal?	Revisión de documentos
	20. Existe un registro de autorización y un registro de salida de los soportes informáticos que contienen información de carácter personal hacia otras dependencias de la empresa u otras entidades.	
Copias de Seguridad y Recuperación de Datos	21. ¿Se realizan copias de seguridad de los datos almacenados en la base de datos?	Entrevista, observación
	21. ¿Existen procedimientos para la realización de copias de seguridad y procedimientos para la restauración del sistema y la recuperación de datos?	Entrevista, observación
	22. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación y restauración de datos garantizan la reconstrucción de estos en el estado en el que se encontraban al tiempo de producirse la pérdida o destrucción de la información.	Entrevista, Observación
	23. ¿Las copias de seguridad se almacenan en dispositivos externos?	
	24. ¿Se verifica que los datos almacenados en soporte externo pueden utilizarse?	Observación
	25. ¿El procedimiento para la restauración de los datos, es conocido sólo por los administradores del sistema o de la base de datos?	Encuesta
	26. ¿Los dispositivos externos en donde se almacenan las copias de seguridad se encuentran ubicados en locales diferentes a donde se encuentran los servidores y redes?	Entrevista
Seguridad Física de los equipos	27. Existe un inventario con la descripción de los equipos informáticos utilizados para el tratamiento de datos (servidores, terminales, ordenadores, etc.)	Revisión de documentos

Etapa de Almacenamiento de Datos		
Derecho de Protección de Datos: Seguridad de Datos		
Factor	**Interrogante**	**Mecanismo**
	28. ¿En el lugar donde están ubicados los servidores y otros dispositivos que almacenen información personal existe un acceso restringido, solo a personal autorizado?	Entrevista, Observación
	29. ¿Hay algún dispositivo o mecanismo de seguridad física en el lugar en donde están ubicados los servidores?	
	30. ¿Se poseen dispositivos extras en el caso de caída o que falle el equipo principal?	
	31. ¿Se cuentan con un generador de energía auxiliar para suministrar corriente eléctrica a los servidores, en caso de algún fallo en el fluido eléctrico?	

4.3.2.9 Guía 9. Utilización de los mecanismos de recolección de información para la etapa de utilización de datos - derecho de protección de datos: datos sensibles

Tabla 42. Descripción de la Guía 9.

Etapa de Utilización de Datos		
Derecho de Protección de Datos: Datos Sensibles		
Factor	**Interrogante**	**Mecanismo**
Publicación de Datos Sensibles	1. Al publicar datos sensibles en páginas Web de su institución, ¿solicita autorización del titular?	Revisión de documento
Soporte informático	2. ¿Se verifica que la salida de soportes informáticos que contienen datos sensibles fuera de la entidad, únicamente podrá ser autorizada por el responsable de los datos en la entidad o en la dependencia?	Entrevista
	3. ¿Se adoptan las medidas necesarias cuando un soporte informático de datos sensibles va a ser desechado o reutilizado de manera que se evite cualquier recuperación de la información almacenada en él previamente?	Entrevista, observación o revisión de documentos
Acceso a datos sensibles	4. ¿Se asegura que solo personal autorizado utilizan y tienen acceso a los datos sensibles, y que están debidamente registrados todos los accesos que se realizan a estos datos a través del sistema?	Consultas al sistema
	5. ¿Se cancelan inmediatamente los derechos de acceso de los usuarios que manejan datos sensibles una vez que cambian de funciones o se desvinculan de la organización?	Entrevista y consulta al sistema

4.3.2.10 Guía 10. Utilización de los mecanismos de recolección de información para la etapa de utilización de datos - derecho de protección de datos: seguridad de datos

Tabla 43. Descripción de la Guía 10.

Etapa de Utilización de Datos		
Derecho de Protección de Datos: Seguridad de Datos		
Factor	**Interrogante**	**Mecanismo**
Funciones y Obligaciones de Personal	1. ¿Existe un manual que define y documenta claramente las funciones y obligaciones del personal, los tipos de acceso y permisos a los sistemas y datos, permitiendo relacionarlos por grupo de usuarios, por perfiles de usuarios o por funciones laborales?	Entrevista y revisión de documentos
	2. ¿Todos los miembros de la entidad tales como trabajadores, administrativos, directivos y demás empleados; tienen conocimiento de sus funciones y obligaciones y su deber de conservar la seguridad en la información que manejan?	Entrevista, encuestas
	3. Dentro de las funciones establecidas en la organización, existe personal informático asignado para: administrar redes, administrar sistemas operativos, administrar bases de datos, operadores de bases de datos y para la aplicación de acceso a las bases de datos, personal de mantenimiento de los sistemas y aplicaciones.	Entrevista
Pruebas con Datos Personales	4. Si es necesario realizar pruebas en el sistema con datos personales ¿Se verifica con anterioridad que el personal encargado tiene la información adecuada y necesaria?	Entrevista y encuesta
	5. ¿Al momento de realizar pruebas con los datos, el personal encargado tiene un plan de prueba que contenga, una descripción del tipo de prueba a realizar, fecha de inicio de la prueba, los recursos a utilizar en las pruebas como, hardware, humanos entre otros y la descripción de pruebas realizadas satisfactoriamente?	Entrevista y revisión de documentos
	6. Si la prueba necesariamente implica tratar datos personales confidenciales ¿se verifica que sean datos no reales, y en el caso que deban ser reales, se asegura que sean eliminados después de finalizada la prueba?	Entrevista

Etapa de Utilización de Datos		
Derecho de Protección de Datos: Seguridad de Datos		
Factor	**Interrogante**	**Mecanismo**
	7. En el caso que la prueba se realice con datos personales confidenciales y reales y no sea posible eliminar los datos ¿se verifica que solo personal autorizado puede realizar las pruebas y que están debidamente registrados todos los accesos que se realizan?	
Planes de Contingencia	8. ¿La organización cuenta con planes de contingencia, que garanticen continuidad y buen funcionamiento en el sistema en caso que ocurra algún imprevisto?	Entrevista, revisión de documentos y encuestas
	9. ¿El personal conoce que la organización dispone de planes de contingencia, si ocurre algún inconveniente?	Entrevista y encuesta
	10. ¿El plan de contingencia identifica todos los posibles riesgos y alternativas o soluciones a los problemas o inconvenientes que se pueden presentar?	Entrevista y revisión de documentos

4.3.2.11 Guía 11. Utilización de los mecanismos de recolección de información para la etapa de utilización de datos - derecho de protección de datos: deber de secreto

Tabla 44. Descripción de la Guía 11.

Etapa de Utilización de Datos		
Derecho de Protección de Datos: Deber de Secreto		
Factor	**Interrogante**	**Mecanismo**
Compromiso de reserva de información	1. ¿Se le informa al administrador de la base datos y a los usuarios del sistema que registran, acceden, procesan y utilizan datos de carácter personal, que están obligados a guardar secreto profesional?	Entrevista y encuesta
	2. ¿Se supervisa a todo el personal que accede a archivos que contienen datos personales, que cumplan con el compromiso de reservar la información contenida en el sistema de información?	
	3. ¿Se ha presentado algún caso donde se infrinja el deber de secreto durante el tratamiento de información de datos personales?	
	4. ¿Se le notifica al personal que accede a la base de datos, las consecuencias de incumplimiento de guardar secreto profesional de los datos personales que se almacenan en el sistema de información?	Entrevista

Etapa de Utilización de Datos		
Derecho de Protección de Datos: Deber de Secreto		
Factor	**Interrogante**	**Mecanismo**
	5. ¿Se sanciona al responsable de la información una vez que incumpla el deber de secreto?	
Autorización limitada a las funciones y actividades a desempeñar	6. ¿El acceso a los datos personales almacenados en las bases de datos, se restringe sólo a personal autorizado, limitado a las funciones y actividades a desempeñar?	Entrevista

4.3.2.12 Guía 12. Utilización de los mecanismos de recolección de información para la etapa de utilización de datos - derecho de protección de datos: comunicación de datos o cesión

Tabla 45. Descripción de la Guía 12.

Etapa de Utilización de Datos		
Derecho de Protección de Datos: Comunicación de Datos o Cesión		
Factor	**Interrogante**	**Mecanismo**
Certificado de Cesión de Datos	1. ¿Cede o comunica datos almacenados en las bases de datos de su organización a terceras personas?	Entrevista
	2. ¿Posee un certificado o documento que compruebe la Cesión?	Revisión de documentos
	3. ¿Se verifica que en este documento está claramente determinada la finalidad de la cesión?	
	4. Al momento de ceder o recibir datos de otro operador certifica o pide certificación en donde el titular de la información ha dado su consentimiento para almacenar, procesar y utilizar sus datos.	Entrevista y revisión de documentos
	5. ¿Se garantiza el correcto uso de los datos de carácter personal durante el tiempo que esté vigente el documento de cesión de acceso a los mismos?	Entrevista
Peticiones de cesión de datos	6. ¿Se resuelven peticiones del titular de la información para su beneficio?	Entrevista
	7. ¿Se atienden las peticiones de cesión de datos acerca de información registrada en bases de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público?	
Control de Cesión de Datos	8. ¿Se le informa al titular de la información de las posibles cesiones a realizar con sus datos?	Entrevista
	9. ¿Se adquiere la autorización del titular de la información para comunicar o ceder sus datos a terceras personas?	Entrevista y revisión de documentos

Etapa de Utilización de Datos		
Derecho de Protección de Datos: Comunicación de Datos o Cesión		
Factor	**Interrogante**	**Mecanismo**
	10. Dentro de las instalaciones de la organización, ¿se lleva control de los datos cedidos a terceros que son procesados en el sistema de información?	
	11. ¿Existen procedimientos formales para controlar la cesión de datos a través de la red?	Entrevista y observación

4.3.2.13 Guía 13. Utilización de los mecanismos de recolección de información para la etapa de utilización de datos - derecho de protección de datos: transferencia internacional

Tabla 46. Descripción de la Guía 13.

Etapa de Utilización de Datos		
Derecho de Protección de Datos: Transferencia Internacional		
Factor	**Interrogante**	**Mecanismo**
Control de Transferencia de Datos	1. ¿Su organización transfiere datos personales almacenados en bases de datos a entidades internacionales o dependencias de gobiernos extranjeros?	Entrevista
	2. Al realizar transferencias internacionales de datos ¿se asegura que el destinatario proporcione las garantías adecuadas para el procesamiento de los datos y utilice la información para fines legales y éticos?	
	3. ¿Se le solicita al responsable de la base de datos o al encargado de la transferencia que aporte documentación complementaria para autorizar dicha transferencia?	Entrevista y revisión de documentos
Registro de Transferencia de Información	4. Al solicitar servicio de alojamiento de datos en un servidor, ¿se asegura que este se encuentra en el lugar donde reside y que dichos datos no son enviados a otro país?	Entrevistas
	5. ¿Se mantiene un registro histórico de la transferencia de archivos ya efectuados y de las empresas que han participado de ellos, donde se especifique la fecha, datos a transferir, nombre del destinatario, finalidad y país?	Entrevistas y revisión de documentos
	6. ¿Se conservan copias de seguridad de los registros que administran la información que es transferida?	Entrevista y observación
Soportes de la Información Transferida	7. Se trasladan soportes de la información transferida fuera de las instalaciones sin la autorización necesaria y sin los controles que se hayan establecido.	Entrevistas

Etapa de Utilización de Datos		
Derecho de Protección de Datos: Transferencia Internacional		
Factor	**Interrogante**	**Mecanismo**
	8. Al momento de transferir datos a otros países ¿Se poseen soportes de la información transferida en la que se pueda verificar el consentimiento del titular del dato?	Entrevistas y revisión de documentos
Convenio de Transferencia	9. ¿Existe un convenio con el país o con la entidad extranjera a donde se van transferir los datos personales, de tal manera que este garantice la protección?	Entrevista y revisión de documentos
	10. ¿En el convenio se define algún periodo de eventos (envíos y reenvíos) de los datos que son transferidos a otro país?	
	11. En el convenio establecido, ¿se le informa al titular de la información que no es necesario solicitar su consentimiento cuando la transferencia sea necesaria para la ejecución o celebración de un contrato, cuando sea necesario proteger el interés público, o sea necesaria la transferencia para la prevención o el diagnóstico médico, entre otros?	
	12. ¿Se transfiere los datos de carácter personal de sus archivos de clientes, proveedores, trabajadores, entre otros, a su empresa matriz con domicilio fuera del país, por motivos de centralización de información, gestión de recursos, procesos de reorganización?	
	13. ¿Se definen en el convenio de transferencia acciones a tomar cuando se sospeche de actividades no autorizadas en la transferencia de los datos?	
Políticas de Seguridad	14. Antes de transferir datos, ¿se asegura de que el país destinatario brinde y garantice niveles de protección adecuados a dichos datos?	Entrevista
	15. ¿Se ejerce vigilancia sobre el destino de los datos que son transferidos?	
	16. Para la transferencia internacional de datos, ¿se establecen procedimientos para reconocer actividades no autorizadas con la información?	Entrevista y revisión de documentos
	17. ¿Se le proporciona al titular información sobre la finalidad del tratamiento y la identidad del responsable del tratamiento de los datos en el tercer país, así como cualquier otra información en la medida en que sea necesaria para garantizar el tratamiento leal?	
	18. ¿Su organización efectúa la transferencia internacional solo a petición del titular de la información o de la organización con la que se tiene convenio?	

4.3.2 Actividad 3. Evaluar el nivel de cumplimiento de los derechos de protección de datos en los procesos seleccionados y diligenciar el formato para evaluar el cumplimiento de los derechos de protección de datos

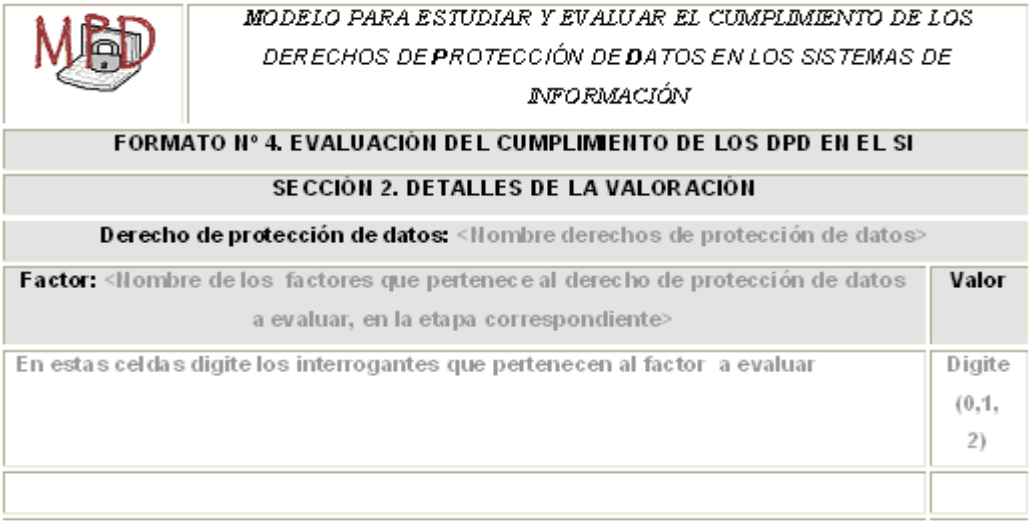
Después de recolectar información a cada uno de los personajes claves en la evaluación, el evaluador debe cotejar la información obtenida de cada persona, para ello debe utilizar el formato Nº 4 (Ver figura16), diligenciando inicialmente detalles de la organización y los derechos que son evaluados por cada etapa, lo anterior se encuentra en la sesión 1 del formato Nº 4; luego se debe dar una valoración a cada interrogante planteado, el cual puede estar entre 0 y 2, tal valoración indica: (0): *No se cumple*, (1): *No se cumple en su totalidad*, (2): *Se cumple,* que se encuentra en la sección 2, del formato Nº 4. Esta sección, debe ser diligenciada por cada derecho de protección de datos.

Después que se haya dado una valoración a cada interrogante, se calcula el promedio por cada factor, por cada derecho de protección de datos y por cada etapa de procesamiento de datos, para determinar sus niveles de cumplimiento, los cuales tienen en cuenta los indicadores y criterios de medición establecidos, *bajo* (0.00 – 0.99), *medio* (1.00 – 1.59) y *alto* (1.60 – 2.00); cabe anotar que los criterios de medición son rangos de los promedios calculados de acuerdo con la valoración estimada a cada interrogante. El promedio y el nivel de cumplimientos de estos componentes del modelo, se registran en la sección 3 del formato Nº 4, la cual debe ser diligenciada para las cuatro etapas del procesamiento de datos definidas.

Figura 16. Formato Nº 4. Evaluación del cumplimiento de los derechos de protección de datos en el sistema de información. Sesión 1.

MPD	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*
FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SESIÓN 1. DETALLES DE LA ORGANIZACIÓN Y DERECHOS A EVALUAR	
Organización: <digite el nombre de la organización que aplicará el modelo>	
Área: <digite el nombre del área o dependencia de la organización que aplicará el modelo>	
Proceso: <digite el nombre del proceso a evaluar>	
Sistema de información: <digite el nombre del sistema de información a evaluar>	
Personal evaluado	
Encuestados:	**Cargo:**
<digite el nombre de las personas que fueron encuestadas>	<digite el cargo de las personas encuestadas>
Evaluadores: <digite el nombre de las personas que realizaron la respectiva evaluación>	
Fecha inicio: <fecha inicio de la evaluación>	**Fecha finalización:** <fecha final de la evaluación >
ETAPA: <Nombre de la etapa>	
Derecho de protección de datos	**Factores**
<En las celdas de esta columna digite los derechos de protección de datos que se evalúan en la etapa>	<En las celdas de esta columna digite los factores de los derechos de protección de datos a evaluar >
VALORACIÓN	
(0): No se cumple	**(1):** No se cumple totalmente / **(2):** Se cumple

Figura 17. Formato Nº 4. Sesión 2. Detalles de la valoración.



MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN	
FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Derecho de protección de datos: <Nombre derechos de protección de datos>	
Factor: <Nombre de los factores que pertenece al derecho de protección de datos a evaluar, en la etapa correspondiente>	**Valor**
En estas celdas digite los interrogantes que pertenecen al factor a evaluar	Digite (0,1, 2)

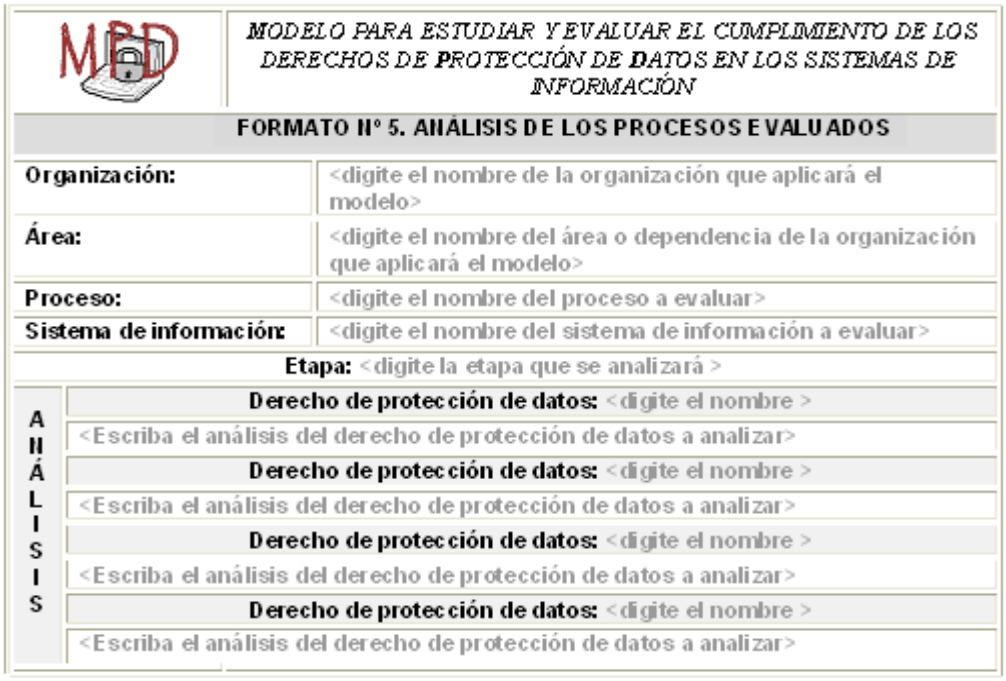
Figura 18. Formato Nº 4. Sesión 3. Detalles de la evaluación.

MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN					
FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI					
SECCIÓN 3. DETALLES DE LA EVALUACIÓN					
SIGLAS					
PCE: Promedio de Cumplimiento Etapa	**PCD:** Promedio de Cumplimiento Derecho	**PCF:** Promedio de Cumplimiento Factor			
NCE: Nivel de Cumplimiento Etapa	**NCD:** Nivel de Cumplimiento Derecho	**NCF:** Nivel de Cumplimiento Factor			
ETAPA				**PCE**	**NCE**
<Nombre de la etapa>					
Derecho de Protección de Datos	**Factor**	**PCF**	**NCF**	**PCD**	**NCD**
<digite los derechos de protección de datos que evaluará en la etapa correspondiente>	<digite los factores que evaluará en los derechos de protección de datos correspondientes>				

4.3.3 Actividad 4. Analizar y esquematizar la situación de los procesos de interés, según los resultados obtenidos en la evaluación del nivel de cumplimiento y graficar estos resultados. Diligenciar formato para analizar los procesos evaluados

En esta actividad se hace un estudio de la información recolectada, en el formato Nº 5 (Ver figura 19), se registra el análisis de la evaluación a cada derecho de protección de datos en los procesos de interés; cabe resaltar, que se utiliza un formato de análisis por cada etapa.

Figura 19. Formato Nº 5. Análisis de lo procesos evaluados.



MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN

FORMATO II° 5. ANÁLISIS DE LOS PROCESOS EVALUADOS

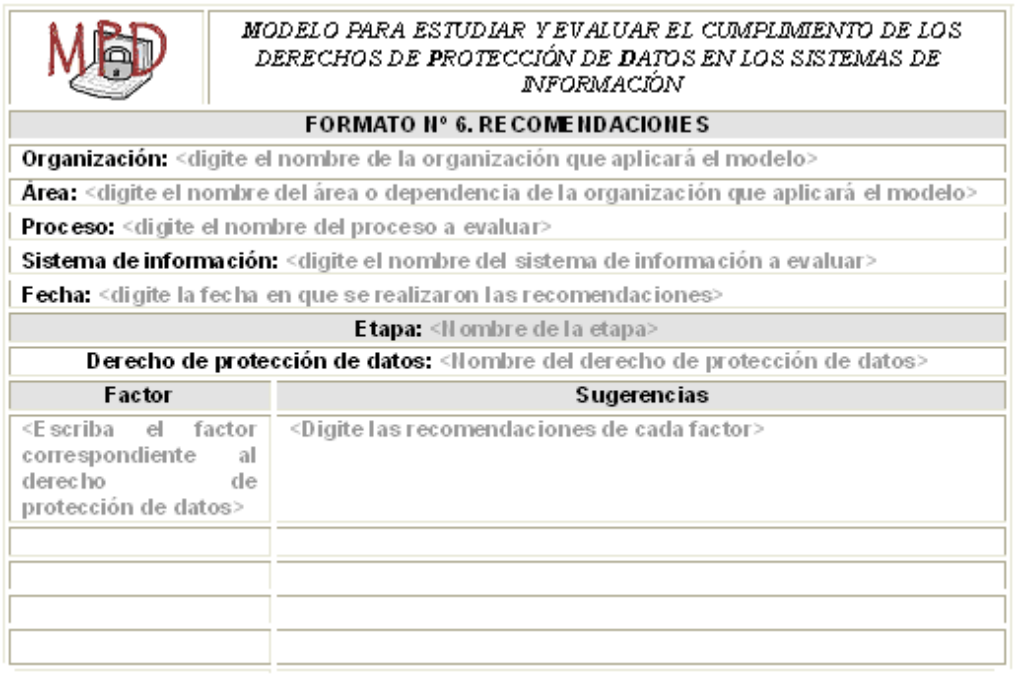
Organización:	<digite el nombre de la organización que aplicará el modelo>
Área:	<digite el nombre del área o dependencia de la organización que aplicará el modelo>
Proceso:	<digite el nombre del proceso a evaluar>
Sistema de información:	<digite el nombre del sistema de información a evaluar>
Etapa: <digite la etapa que se analizará >	
ANÁLISIS	**Derecho de protección de datos:** <digite el nombre >
	<Escriba el análisis del derecho de protección de datos a analizar>
	Derecho de protección de datos: <digite el nombre >
	<Escriba el análisis del derecho de protección de datos a analizar>
	Derecho de protección de datos: <digite el nombre >
	<Escriba el análisis del derecho de protección de datos a analizar>
	Derecho de protección de datos: <digite el nombre >
	<Escriba el análisis del derecho de protección de datos a analizar>

4.3.4 Actividad 5. Formular el estado y las recomendaciones de los procesos organizacionales seleccionados y su sistema de información con respecto al cumplimiento de los derechos de protección de datos. Diligenciar formato de recomendaciones

En esta fase, el evaluador debe formular el estado en el que se encuentra el sistema de información que sirve de apoyo para los procesos evaluados, con

respecto el cumplimiento de los derechos de protección de datos, estos resultados deben ser mostrados por medio de una gráfica; en la Figura 20 se presenta el formato Nº 6, este se utiliza para formular las recomendaciones a las falencias encontradas en el proceso durante la evaluación, si el administrador del sistema de información que utiliza datos personales decide implementar estas medidas, se garantiza el derechos de habeas data al titular de los datos. Estas sugerencias serán dadas por factores, teniendo en cuenta que cada factor trata puntos diferentes; de esta manera se utiliza un formato de recomendaciones por cada derecho de protección de datos.

Figura 20. Formato Nº 6. Recomendaciones.



MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN	
FORMATO Nº 6. RECOMENDACIONES	
Organización: <digite el nombre de la organización que aplicará el modelo>	
Área: <digite el nombre del área o dependencia de la organización que aplicará el modelo>	
Proceso: <digite el nombre del proceso a evaluar>	
Sistema de información: <digite el nombre del sistema de información a evaluar>	
Fecha: <digite la fecha en que se realizaron las recomendaciones>	
Etapa: <Nombre de la etapa>	
Derecho de protección de datos: <Nombre del derecho de protección de datos>	
Factor	**Sugerencias**
<Escriba el factor correspondiente al derecho de protección de datos>	<Digite las recomendaciones de cada factor>

4.3.5 Actividad 6. Monitorear de 1 a 5 y llevar a cabo acción control

En esta actividad se realiza un monitoreo de la ejecución de todas las actividades anteriores y se toman las acciones correctivas necesarias para mejorar la ejecución de estas actividades.

Las anteriores son las actividades necesarias para desarrollar y aplicar el proyecto planteado. Para que el lector comprenda un poco más el modelo

anteriormente diseñado y la forma como este estudia y evalúa a los sistemas de información que sirven de apoyo a los procesos que manejan información personal, el siguiente capítulo expone la experiencia de la aplicación del modelo de protección de datos al caso de estudio seleccionado.

5 APLICACIÓN DEL MODELO - CASO DE ESTUDIO LA DEPENDENCIA DE ADMISIONES, REGISTRO Y CONTROL ACADÉMICO DE LA UNIVERSIDAD DEL MAGDALENA

En este capítulo se realiza una descripción del sistema de información de la dependencia de Admisiones, Registro y Control Académico, de la Universidad del Magdalena, luego se realiza un estudio de los procesos organizacionales de esta, se prosigue a evaluar el nivel de cumplimiento de los derechos de protección de datos en el proceso seleccionado y se analizan los resultados obtenidos; posteriormente se formula el estado actual del proceso evaluado y se plantean recomendaciones para cumplir satisfactoriamente estos derechos.

5.1 DESCRIPCIÓN DEL SISTEMA DE INFORMACIÓN DEL CASO DE ESTUDIO – DEPENDENCIA DE ADMISIONES, REGISTRO Y CONTROL ACADÉMICO

La Universidad del Magdalena es una institución que se encuentra organizada en dependencias, dentro de las cuales se tomó como caso de estudio la dependencia Admisiones, Registro y Control Académico (ARCA), que posee un sistema de información llamado "*Sistema Integrado de Liquidación, Admisiones, Registro y Control Académico*", el cual tiene las siguientes características:

- Diseño modular y parametrizado
- Ambiente Windows
- Procesos en línea.
- Ayuda contextual y HTML
- Ambiente Cliente – Servidor
- Sistema de información desarrollado en ORACLE 9i Forms
- Aplicaciones Web desarrolladas en JSP

El sistema de información presenta tres módulos: matrícula y registro, administración del sistema y formación académica.

El módulo de “Matrícula y registro”, posee funciones para el manejo de la admisión de un estudiante, liquidación económica por concepto de derechos de matrícula de cada estudiante en un semestre, administrar la hoja de vida de un estudiante, realizar matrículas académicas, y elaborar estadísticas.

El módulo de “Administración del sistema”, presenta funciones para realizar copias de seguridad y para mantener auditorías.

El módulo de “Formación académica”, reúne funciones relacionadas con la administración de la planta física, programación de un período académico y el mantenimiento de los planes de estudio implantados en los programas de la Universidad.

5.2 ACTIVIDADES PARA LA APLICACIÓN DEL MODELO AL CASO DE ESTUDIO DE ARCA

En esta sección se presenta el desarrollo del conjunto de actividades definidas en el capítulo 4, las cuales son las necesarias para estudiar y evaluar el cumplimiento de los derechos de protección de datos en el caso de estudio señalado.

5.2.1 Analizar los procesos organizacionales que manejan información personal y son apoyados por SI/TI

En esta primera fase de aplicación del modelo, se observó a la dependencia en general, se realizó el primer contacto con el director de ARCA, quien colaboró con la disposición del personal que opera en el sistema de información datos personales, además, asignó un horario para la recolección de la información.

5.2.1.1 Seleccionar los procesos a evaluar

La dependencia de ARCA desarrolla tres procesos básicos, los cuales manejan información personal y tienen apoyo de SI/TI, los cuales son el de admisión de aspirantes, registro y control académico, y expedición de certificados, los tres se realizan en la modalidad de presencial y a distancia, que se desarrollan por separado; aunque los tres procesos desarrollados en la dependencia cumplen con las condiciones necesarias, los desarrolladores de este proyecto de investigación han seleccionado el proceso de *Admisión de aspirantes en los programas de pregrado presencial* para ilustrar la aplicación del modelo de protección de datos (Ver Tabla 47).

Tabla 47. Formato Nº 1. Proceso seleccionado a evaluar

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

Formato Nº 1. Selección de procesos a evaluar			
Organización:	Universidad de Magdalena		
Área:	Admisiones, Registro y Control Académico – ARCA		
Responsable:	Ingeniero Samuel Prieto Mejía		
Proceso	**Manejo información personal**	**Apoyo SI/TI**	**Proceso seleccionado**
Admisión de aspirantes en los programas de pregrado presencial	**X**	**X**	**X**
Registro y control académico en los programas de pregrado presencial	**X**	**X**	
Admisión de aspirantes en los programas de pregrado a distancia	**X**	**X**	
Registro y control académico en los programas de pregrado a distancia	**X**	**X**	
Expedición de certificados	**X**	**X**	

5.2.1.2 Analizar las actividades del proceso a evaluar

Después de seleccionar el proceso de admisión de aspirantes en los programas de pregrado presencial para ilustrar la aplicación del modelo, se consultó con el personal que lleva a cabo el desarrollo de este proceso, y con su apoyo se definieron las actividades, descripción y responsables de cada una de ellas, que permitió comprender el funcionamiento del proceso e identificar el personal que interviene en cada una de las etapas del procesamiento de datos (Ver Tabla 48).

Tabla 48. Formato 2. Aplicación caso de estudio

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*		
Formato Nº 2. Análisis para las actividades del proceso a evaluar			
Organización:	Universidad del Magdalena		
Área:	Admisiones Registro Y Control Académico – ARCA		
Proceso:	Admisión de aspirantes en los programas de pregrado presencial		
Sistema de Información:	Sistema de información de ARCA		
Fecha:	3 - julio – 2008		
Nº	**Actividades**	**Descripción**	**Responsable**
1.	Generar volante de consignación	El aspirante, por medio del sistema genera el volante de consignación para el pago de la inscripción.	Coordinador de inscripción
2.	Activar consignación	Después de 24 horas es activa la consignación, para luego realizar la inscripción.	Coordinador de inscripción
3.	Recibir inscripción en línea	Extrae del sistema de información las inscripciones realizadas por los usuarios, a través del aplicativo Web	Coordinador de inscripción
4.	Generar informe diario de inscritos	Por medio del sistema se realiza un informe diario de los inscritos.	Coordinador de inscripción
5.	Recibir documentación	Revisa los documentos soportes requeridos para legalizar la inscripción.	Atención al público
6.	Elaborar informe de inscripción	Consulta y extrae del sistema de información los datos de todos los aspirantes inscritos para el periodo académico.	Coordinador de inscripción
7.	Comunicar informe	Revisa la información suministrada por el coordinador de inscripción, realiza ajustes si es necesario y	Director de Admisiones Registro y Control Académico

		envía informe a los interesados.	
8.	Recibir información y credenciales	Recibe información para la realización del examen de admisión y las credenciales para identificar a cada aspirante hasta que sea admitido.	Director de Admisiones Registro y Control Académico
9.	Comunicar credenciales	Envía al correo electrónico de cada aspirante la credencial de identificación.	Coordinador de inscripción
10.	Recibir información	Recibe la información de los resultados de los exámenes de admisión.	Director de Admisiones Registro y Control Académico
11.	Seleccionar admitidos	Con base en los resultados de la prueba de admisión, el sistema procesa la información para definir los nuevos admitidos, lista de espera, cupos especiales, exoneraciones, nivelatorio, etc. Se organiza el listado de admitidos en cada programa académico.	Coordinador de selección de estudiantes
12.	Publicar admitidos	Publica en la página Web de la Universidad del Magdalena el listado de los nuevos estudiantes admitidos	Coordinador de inscripción
13.	Asignar códigos	Por medio del sistema se asigna un código de identificación al admitido y se aplican las exoneraciones según los acuerdos y reglamentos establecidos.	Coordinador de selección de estudiantes
14.	Activar liquidaciones de matrícula	Se generan las liquidaciones de matrícula teniendo en cuenta el listado de cupos especiales y exoneraciones.	Coordinador de registro y control académico.
15.	Activar matrícula académica	Después del pago, el nuevo admitido puede realizar la matrícula académica según los horarios establecidos.	Coordinador de registro y control académico
16.	Elaborar informe de matrícula financiera	Consulta y extrae del sistema de información datos solicitados por el director de la división, con relación a las actividades del periodo de matricula financiera.	Coordinador de registro y control académico
17.	Comunicar informe	Revisa la información suministrada por el coordinador financiero y envía informe a los interesados.	Director de admisiones, registro y control académico

5.2.1.3 Seleccionar el personal clave para la evaluación

De acuerdo a la actividad anteriormente realizada, en esta se hizo una clasificación del personal que interviene en cada etapa del procesamiento de los datos y según el criterio y el análisis realizado al proceso de *admisión de aspirantes en los programas de pregrado presencial,* se ha seleccionado como el personal más apropiado para la evaluación, los clasificados por cada etapa y el administrador de la base de datos del sistema de información de ARCA, mostrados en el formato Nº 3. (Ver Tabla 49); en este caso se han unido las etapas de procesamiento y almacenamiento, porque en ambas, interviene el mismo personal.

Tabla 49. Formato Nº 3. Personal clave para la evaluación

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*	
FORMATO Nº 3. PERSONAL CLAVE PARA LA EVALUACIÓN		
Organización:	Universidad del Magdalena	
Área:	Admisiones Registro y Control Académico - ARCA	
Proceso:	Admisión de aspirantes en los programas de pregrado presencial	
Sistema de información:	Sistema de información de ARCA	
Fecha:	8 de julio 2008	
Etapa procesamiento de datos	**Personal clave para la evaluación**	**Nombre**
Recolección y Registro	Coordinador de inscripción	Jaider Ariza
Procesamiento	Administrador base de datos	Álvaro Gamarra
	Coordinador de registro y control académico	Wilmer Rueda
	Coordinador de selección de estudiantes	Jhon Martínez
Almacenamiento Y Utilización	Administrador base de datos	Álvaro Gamarra
	Coordinador de registro y control académico	Wilmer Rueda

5.2.2 Recolectar información aplicando los mecanismos de recolección definidos en la guía de utilización de mecanismos de recolección de información, en cada etapa del proceso seleccionado

Después de seleccionar el proceso y clasificar al personal para la evaluación, en esta actividad se procedió a recolectar información. Esta labor se inició con una exploración a la guía de utilización de los mecanismos de recolección de información y se personalizaron estos formatos generales a la condición de la dependencia de ARCA, en conjunto con otras actividades las cuales se muestran en detalle a continuación:

5.2.2.1 Seguir pautas de la guía de utilización de los mecanismos de recolección de información

Para no recolectar información errónea o que no aplique para el proceso de interés, se hizo una revisión a la guía de utilización de los mecanismos de recolección de información, para poder definir qué derechos de protección de datos son los pertinentes para la evaluación.

5.2.2.2 Personalizar los formatos generales de los mecanismos de recolección de información, de acuerdo a la situación percibida en la dependencia de ARCA

El modelo de protección de datos está diseñado para cualquier organización, en este caso los evaluadores personalizaron los formatos generales de recolección de información de acuerdo a las actividades realizadas en el proceso evaluado; es decir, solo se evaluaron los interrogantes, factores o derechos de protección de datos que aplican para la dependencia; en la Tabla 50 se muestran cada uno de los componentes y el motivo, por el cual estos no se evaluaron para el proceso de *admisión de estudiantes en el programa de pregrado presencial.*

Tabla 50. Componentes a no evaluar en el caso de estudio

Etapa	Derechos de protección de datos	Factor	Nº Interrogante	Razón
Recolección y registro de datos	Información en la recogida de datos	Procedimiento de recogida de datos personales	3	La entidad recolecta los datos directamente del titular
Almacenamiento de datos	Calidad de datos	Redundancia de datos	8, 9 y 10	La base de datos está diseñada para no presentar redundancia de datos.
	Seguridad de datos	Cambios en la estructura de la base de datos	Todos	No se realizan modificaciones a la estructura de la base de datos
Utilización de datos	Datos sensibles	Soporte informático	3	Los soportes informáticos que contienen datos no se desechan ni se reutilizan, todos son almacenados.
	Transferencia internacional de datos	Todos	Todos	En el desarrollo del proceso no se envían datos personales de los aspirantes hacia otros países

5.2.2.3 Aplicar los mecanismos de recolección de información correspondientes a cada etapa del proceso seleccionado.

En esta etapa, se entrevistó al personal seleccionado para realizar la evaluación, los cuales fueron descritos en la Tabla 49, Formato Nº 3. La información se recolectó por medio de los mecanismos de recolección de información definidos en el capítulo 2, al personal seleccionado para la evaluación se le realizaron entrevistas, de igual forma se revisaron documentos en medio físico y magnético, observaciones y consultas al sistema para verificar la información proporcionada por cada una de las personas entrevistadas.

En los formatos de evaluación (Ver Tabla 54-57) se muestran los derechos de protección de datos y factores que se evaluaron y la recopilación de la información

obtenida al aplicar los mecanismos de recolección a cada etapa del proceso de *admisión de estudiantes en el programa de pregrado presencial.*

5.2.2.4 Revisar si los mecanismos utilizados recolectaron la información necesaria para evaluar el cumplimiento de los derechos de protección de datos en el sistema de información.

Cuando se entrevistó a todo el personal seleccionado, se revisaron los documentos y se realizaron las consultas al sistema, se analizó la información obtenida para conocer si estos mecanismos recolectaron la información necesaria para la evaluación, en el caso de estudio, no hubo necesidad de cambiar o incluir un mecanismo mas, ya que los utilizados en cada interrogante fueron suficientes para obtener información y realizar la evaluación.

5.2.3 Evaluar el nivel de cumplimiento de los derechos de protección de datos en el proceso seleccionado

En esta actividad se diligencia el formato para evaluar el cumplimiento de los derechos de protección de datos, que de acuerdo a la información dada por cada uno de los entrevistados, la observación y la revisión de documentos realizados se dio una valor a la calificación de cada interrogante planteado, el cual puede estar entre 0 y 2 (Ver Tabla 51).

Tabla 51. Indicadores para evaluar cada interrogante planteado

Nivel de control	Descripción
2	Se cumple
1	No se cumple totalmente
0	No se cumple

Para evaluar el nivel de cumplimiento en los derechos de protección de datos, los desarrolladores de la investigación propusieron las siguientes fórmulas:

PCD - Promedio de Cumplimiento del Derecho = [((Σ calificación de cada interrogante factor1/Nº de interrogantes factor1) + (Σ calificación de cada interrogante factor2/Nº de interrogantes factor2) +…… + (Σ calificación de cada interrogante factorN/Nº de interrogantes factorN))/ Nº de factores del derecho]

Donde, Σ indica la adición de la calificación de cada interrogante de los factores del derecho, dividido por el número de factores del derecho.

Para hallar el promedio de cumplimiento en la etapa, se utiliza la fórmula:
PCE - Promedio de Cumplimiento de la Etapa = ((Σ PCD)/Nº de derechos de protección de datos evaluados en la etapa)

Donde Σ indica la sumatoria de los promedios de los derechos de protección de datos evaluados en una etapa, dividido por el número de derechos de protección de datos de la etapa.

Para una mejor comprensión, se cita un ejemplo que muestra como es la forma de evaluación. Se tiene la etapa1, a la cual pertenecen los derechos de protección de datos A y B. El derecho de protección de datos A posee los factores 1A y 2A, y el derecho B los factores 1B y 2B la calificación para los interrogantes de cada factor se muestra en la Tabla 52.

Tabla 52. Ejemplo para calcular nivel de cumplimiento

Etapa: 1	
Derecho de protección de datos: A	
Factor: 1A	**Valor**
1. Interrogante 1	**2**
2. Interrogante 2	**2**
3. Interrogante 3	**1**
Factor: 2A	**Valor**
4. Interrogante 1	**0**
5. Interrogante 2	**1**
Derecho de protección de datos: B	

Factor: 1B	Valor
6. Interrogante 1	**2**
7. Interrogante 2	**2**
Factor: 2B	**Valor**
8. Interrogante 1	**1**
9. Interrogante 2	**2**
10. Interrogante 3	**0**

Para hallar el nivel de cumplimiento de los derechos de protección de datos, inicialmente se utiliza la fórmula para calcular el Promedio de Cumplimiento del Derecho:

PCD = [((Σ calificación de cada interrogante factor1/Nº de interrogantes factor1) + (Σ calificación de cada interrogante factor2/Nº de interrogantes factor2) +…… + (Σ calificación de cada interrogante factorN/Nº de interrogantes factorN))/ Nº de factores del derecho]

Remplazando la formula para el derecho A, se tiene:

PCD (A) = [(((2+2+1)/3) + ((0+1)/2))/ 2]

PCD (A) = [(1.66 + 0.50) / 2]

PCD (A) = 1.08

De estos cálculos se puede determinar el nivel de cumplimiento de los factores

PCF (1A) = 1.66

PCF (2A) = 0.50

Posteriormente se puede calcular el Promedio de Cumplimiento del Derecho B

PCD (B) = [((2+2)/2) + (1+2+0)/3)) / 2]

PCD (B) = [(2 + 1)/2]

PCD (B) = 1.50

Entonces, para los factores de este derecho se tiene,

PCF (1B) = 2

PCF (2B) = 1

Posteriormente se evalúa el Promedio de Cumplimiento de la Etapa

PCE = [(Σ PCD)/Nº de derechos de protección de datos evaluados en la etapa]

PCE (1) = [(1.08 + 1.50)/2]

PCE (1) = 1.29

Al calcular los promedios de cumplimiento en una etapa, estos deben ser comparados con los indicadores de la Tabla 29 del Capítulo 4 y dependiendo en el rango en que estén comprendidos, se determina el nivel de cumplimiento, para los factores, los derechos y la etapa.

Luego de comparar los promedios obtenidos con los criterios de medición, se determinó el nivel de cumplimiento para cada uno de los componentes, los cuales son mostrados en la Tabla 53.

Tabla 53. Resultados de la evaluación del ejemplo

ETAPA				**PCE**	**NCE**
Etapa 1				1.29	Medio
Derecho de Protección de Datos	**Factor**	**PCF**	**NCF**	**PCD**	**NCD**
Derecho A	Factor 1A	1.66	Alto	1.08	Medio
	Factor 2A	0.50	Bajo		
Derecho B	Factor 1B	2.00	Alto	1.50	Medio
	Factor 2B	1.00	Medio		

Después de presentar las fórmulas utilizadas en la evaluación, las Tablas (54-57) muestran el valor de la calificación dada a cada interrogante y el nivel de cumplimiento de los derechos de protección de datos en las cuatro etapas definidas para el procesamiento de datos en el sistema de información de ARCA, que es el sistema que apoya el proceso de Admisión de aspirantes en los programas de pregrado presencial.

Tabla 54. Evaluación del cumplimiento de los derechos de protección de datos en la etapa de recolección y registro de datos

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*
FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 1. DETALLES DE LA ORGANIZACIÓN Y DERECHOS A EVALUAR	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico - ARCA
Proceso:	Admisión de aspirantes en los programas de pregrado presencial
Sistema de información:	Sistema de información de ARCA
Personal evaluado	
Encuestados:	**Cargo:**
Ingeniero Jaider Ariza	Coordinador de inscripción
Evaluadores	
Ivonne Cabarcas Herrera, Elsy Cantillo Cabarcas, Vanesa Viloria Machado	
Fecha inicio: 4 Julio 2008	**Fecha finalización:** 7 julio 2008
Etapa: Recolección y registro de datos	
Derecho de protección de datos	**Factores**
Calidad de Datos	Redundancia de Datos
	Control de entradas en campos
	Seguimiento de la información
Información en la Recogida de Datos	Procedimiento de recogida de datos personales
	Documento de soporte
	Finalidad
Consentimiento	Autorización del titular del dato
	Procedimiento de publicación de datos personales
Datos Sensibles	Autorización para la Administración de Datos Sensibles
Valoración	
(0): No se cumple	**(1):** No se cumple totalmente **(2):** Se cumple

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Recolección y registro de datos	
Derecho de protección de datos: Calidad de Datos	
Factor: Redundancia de datos	**Valor**
1. Al recolectar datos, ¿se verifica que en las diferentes áreas de la organización no estén recolectando de manera independiente la misma información?	**2**
2. ¿Los datos personales recolectados y registrados en el sistema de información son almacenados en una misma base de datos para toda la organización?	**2**
Factor: Control de entradas en campos	**Valor**
3. ¿El ingreso de datos a los campos de la base de datos se realiza con previa autorización?	**2**
4. Al registrar datos en los sistemas de información, ¿verifica que los datos ingresados correspondan con el campo indicado en la base de datos?	**2**
5. ¿Se lleva a cabo un control detallado de los datos que se registran en los campos de la base de datos?	**1**
6. ¿Al registrar los datos en el sistema de información, poseen controles para que en cada campo se digite el formato (número o letra) y el tamaño adecuado?	**2**
7. ¿Al registrar datos, se tiene control sobre la entrada de los campos obligatorios, para que no sean llenados en blanco?	**2**
8. ¿Se tiene un rango máximo y mínimo al número de caracteres o dígitos a digitar en cada campo?	**2**
9. ¿En el sistema se realiza una prenumeración de formatos para el ingreso de datos o registros de transacciones? ¿El sistema controla la secuencia de los formatos prenumerados?	**0**
Factor: Seguimiento de la información	**Valor**
10. ¿Se definen los medios para recolectar la información antes de que los datos sean almacenados en una base de datos, de manera que estos no sean recolectados por medios desleales o fraudulentos?	**2**
11. Al recolectar y registrar datos personales en los sistemas de información, ¿se asegura que sean reales, completos y actualizados?	**2**

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Recolección y registro de datos	
Derecho de protección de datos: Información en la recogida de datos	
Factor: Procedimiento de recogida de datos personales	**Valor**
1. ¿Al titular de los datos se le ha informado de forma expresa, precisa y clara de los siguientes aspectos?	
1.1. De la creación de una base de datos propiedad de la entidad donde serán almacenados sus datos personales	**0**
1.2. Del propósito de la recogida de los datos, la finalidad para la que serán tratados y quienes pueden ser los destinatarios de la información.	**0**
1.3. Del carácter obligatorio o facultativo de suministrar los datos que le sean solicitados, y las consecuencias de proporcionar datos no exactos o falsos al momento de recolectar la información.	**0**
1.4. De la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición de los datos que serán almacenados en bases de datos.	**2**
2. ¿Su entidad recolecta los datos directamente del titular de la información?	**2**
3. Si la anterior respuesta es negativa, ¿dispone de algún método para informarle de este hecho y de la fuente de la que provienen los datos?	**NAP**
Factor: Documento de Soporte	**Valor**
4. Al momento de recolectar y registrar datos personales en bases de datos, ¿solicita una autorización por escrito o posee formatos firmados por el titular, en donde se evidencie que proporciona sus datos personales de manera voluntaria?	**0**
5. Si su organización utiliza documentos, cuestionarios, formularios impresos o electrónicos u otros mecanismos de recogida y registro de datos online ¿incluyen en estos, información sobre el tratamiento y la finalidad de la recogida de estos datos y los posibles destinatarios de la información?	**0**
6. ¿De los documentos recolectados existe en el sistema de información un registro de estos?	**0**
Factor: Finalidad	**Valor**
7. ¿Los datos de carácter personal almacenados en la base de datos guardan directa relación con la finalidad legal para la cual se recolectan?	**2**

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Recolección y registro de datos	
Derecho de protección de datos: Consentimiento	
Factor: Autorización del titular del dato	**Valor**
4. Al recolectar y registrar datos personales en bases de datos, ¿Su entidad solicita el consentimiento expreso y por escrito al titular para tratar estos datos, ya sea un documento o formularios empleados en la recogida de datos con cláusulas de consentimiento y firmados por el titular?	**0**
Factor: Procedimiento de publicación de datos personales	**Valor**
5. En el momento de registrar datos, ¿el área o dependencia solicita el consentimiento del titular de la información para publicar sus datos en páginas Web?	**0**
6. Si su entidad recolecta datos online, ¿posee formularios con cláusulas o políticas de seguridad, en donde le indique al titular que debe dar el consentimiento para que sus datos puedan ser almacenados y tratados en una base de datos propiedad de la organización?	**0**
Derecho de protección de datos: Datos sensibles	
Factor: Autorización para la administración de datos sensibles	**Valor**
Si su organización recolecta y registra en sus bases de datos, datos sensibles, como son los referentes a origen racial y étnico, ideología, afiliación sindical, religión, opiniones políticas, creencias, salud, o vida sexual.	
3. Al recolectar datos sensibles ¿Se solicita el consentimiento previo por escrito del titular para registrar y tratar estos datos en sistemas de información de su organización?	**0**
4. Antes de registrar datos personales en bases de datos, ¿se le informa al titular de los datos del derecho a no declarar sobre su ideología, religión o creencias?	**0**

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI

SECCIÓN 3. DETALLES DE LA EVALUACIÓN

Siglas

PCE: Promedio de Cumplimiento Etapa	**PCD:** Promedio de Cumplimiento Derecho	**PCF:** Promedio de Cumplimiento Factor
NCE: Nivel de Cumplimiento Etapa	**NCD:** Nivel de Cumplimiento Derecho	**NCF:** Nivel de Cumplimiento Factor

ETAPA	PCE	NCE
Recolección y registro de datos	**0.69**	**Bajo**

Derecho de Protección de Datos	Factor	PCF	NCF	PCD	NCD
Calidad de datos	Redundancia de Datos	**2.00**	**Alto**	**1.85**	**Alto**
	Control de Entradas en Campos	**1.57**	**Medio**		
	Seguimiento de la Información	**2.00**	**Alto**		
Información en la Recogida de Datos	Procedimiento de Recogida de Datos Personales	**0.80**	**Bajo**	**0.93**	**Bajo**
	Documento de Soporte	**0.00**	**Bajo**		
	Finalidad	**2.00**	**Alto**		
Consentimiento	Autorización del Titular del Dato	**0.00**	**Bajo**	**0.00**	**Bajo**
	Procedimiento de publicación de datos personales	**0.00**	**Bajo**		
Datos Sensibles	Autorización para la Administración de Datos Sensibles	**0.00**	**Bajo**	**0.00**	**Bajo**

Tabla 55. Evaluación del cumplimiento de los derechos de protección de datos en la etapa de procesamiento de datos

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI		
SECCIÓN 1. DETALLES DE LA ORGANIZACIÓN Y DERECHOS A EVALUAR		
Organización:	Universidad del Magdalena	
Área:	Admisiones Registro y Control Académico – ARCA	
Proceso:	Admisión de aspirantes en los programas de pregrado presencial	
Sistema de información:	Sistema de información de ARCA	
Personal evaluado		
Encuestados:	**Cargo:**	
Ingeniero Álvaro Gamarra	Administrador base de dato	
Ingeniero Wilmer Rueda	Coordinador de control y registro académico	
Ingeniero Jhon Mario Martínez	Coordinador selección de estudiantes	
Evaluadores		
Ivonne Cabarcas Herrera, Elsy Cantillo Cabarcas, Vanesa Viloria Machado		
Fecha inicio: 15 Julio 2008	**Fecha finalización:** 17 de julio 2008	
Etapa: Procesamiento de datos		
Derecho de protección de datos	**Factores**	
Seguridad de los datos	Identificación y autenticación	
	Control de acceso	
	Restauración de datos	
Valoración		
(0): No se cumple	**(1):** No se cumple totalmente	**(2):** Se cumple

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Procesamiento de datos	
Derecho de protección de datos: Seguridad de datos	
Factor: Identificación y autenticación	**Valor**
1. ¿La base de datos donde se almacenan los datos personales está protegida por contraseña?	**2**
2. ¿El administrador de la base de datos y los usuarios tienen contraseñas para acceder al sistema de información?	**2**
3. Si el administrador del sistema crea cuentas a los usuarios, ¿estos se encargar de generar sus contraseñas?	**2**
4. ¿Los usuarios y el administrador de la base de datos cambian periódicamente las contraseñas o claves de acceso a los sistemas?	**0**
5. ¿Las contraseñas utilizadas para acceder a los sistemas tienen definida una longitud mínima y contiene requisitos de complejidad, tales como números o letras?	**1**
6. ¿Al establecer las contraseñas, los usuarios pueden repetir las últimas contraseñas utilizadas?	**0**
7. ¿Poseen las contraseñas un tiempo máximo de vigencia, y es obligatorio que se cambien las contraseñas de acceso a los sistemas después de pasado este periodo de vigencia?	**0**
8. ¿Existen procedimientos de bloqueo y desbloqueos de cuenta por utilización reiterada de contraseñas incorrectas?	**0**
9. ¿Se registran los nombres de usuarios y contraseñas de los accesos no autorizados o rechazados a las estructuras, tablas lógicas y tablas físicas de la base de datos?	**0**
10. ¿Las contraseñas de acceso son almacenadas de forma no legible?	**2**

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Procesamiento de datos	
Derecho de protección de datos: Seguridad de datos	
Factor: Control de acceso	**Valor**
11. ¿En la empresa o dependencia existe un administrador de sistemas que gestiona y controla los perfiles de usuarios?	**2**
12. ¿Se controla el acceso de los usuarios a los datos y recursos como sistemas, equipos, programas, aplicaciones, bases de datos, redes, etc, de acuerdo a sus funciones laborales?	**2**
13. ¿En los sistemas se puede identificar y auditar los accesos y acciones realizados por cada usuario?	**2**
14. ¿Se tiene una lista o tabla actualizada en la base de datos de los usuarios que acceden a los sistemas de información, así como de los usuarios autorizados a acceder y procesar datos en cada uno de los módulos del sistema y sus bases de datos?	**2**
15. ¿Para los accesos a través de redes de telecomunicaciones, se adoptan las mismas medidas que para los accesos locales?	**2**
Factor: Restauración de datos	**Valor**
16. Al procesar datos personales, ¿existen mecanismos que al reiniciar la ejecución de un proceso interrumpido permitan continuar con el procesamiento de los datos sin repetir o sin dejar de procesar algunas operaciones?	**0**
17. Si la anterior respuesta es positiva, al procesar datos personales, ¿los procedimientos establecidos para la recuperación y restauración de datos garantizan la reconstrucción de estos en el estado en el que se encontraban al tiempo de producirse un fallo en el sistema?	**0**

MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI

SECCIÓN 3. DETALLES DE LA EVALUACIÓN

Siglas

PCE: Promedio de Cumplimiento Etapa	**PCD:** Promedio de Cumplimiento Derecho	**PCF:** Promedio de Cumplimiento Factor
NCE: Nivel de Cumplimiento Etapa	**NCD:** Nivel de Cumplimiento Derecho	**NCF:** Nivel de Cumplimiento Factor

ETAPA	PCE	NCE
Procesamiento de datos	**0.96**	**Bajo**

Derecho de protección de datos	Factor	PCF	NCF	PDC	NCD
Seguridad de datos	Identificación y autenticación	**0.90**	**Bajo**	**0.96**	**Bajo**
	Control de acceso	**2.00**	**Alto**		
	Restauración de datos	**0.00**	**Bajo**		

Tabla 56. Evaluación del cumplimiento de los derechos de protección de datos en la etapa de almacenamiento de datos

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI		
SECCIÓN 1. DETALLES DE LA ORGANIZACIÓN Y DERECHOS A EVALUAR		
Organización:	Universidad del Magdalena	
Área:	Admisiones Registro y Control Académico – ARCA	
Proceso:	Admisión de aspirantes en los programas de pregrado presencial	
Sistema de información:	Sistema de información de ARCA	
Personal evaluado		
Encuestados	**Cargo**	
Ingeniero Álvaro Gamarra	Administrador de servidores	
Ingeniero Wilmer Rueda	Coordinador de control y registro académico	
Evaluadores:		
Ivonne Cabarcas Herrera, Elsy Cantillo Cabarcas, Vanesa Viloria Machado		
Fecha inicio: 8 de julio 2008	**Fecha finalización:**	
Etapa: Almacenamiento de datos		
Derecho de protección de datos	**Factores**	
Calidad de datos	Actualización de datos	
	Seguimiento de la información	
	Redundancia de datos	
Datos sensibles	Registro de operación de los datos	
Seguridad de datos	Medidas técnicas de seguridad	
	Documentación de los sistemas de información	
	Estructura de las bases de datos	
	Cambios en la estructura de las bases de datos (NAP)	
	Registro de incidencias	
	Gestión de soporte	
	Copias de seguridad y recuperación de datos	
	Seguridad física de los equipos	
Valoración		
(0): No se cumple	**(1):** No se cumple totalmente	**(2):** Se cumple

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*	
FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI		
SECCIÓN 2. DETALLES DE LA VALORACIÓN		
Etapa: Almacenamiento de datos		
Derecho de protección de datos: Calidad de datos		
Factor: Actualización de datos		**Valor**
1.	¿Se le ha presentado algún evento en el que maneje datos personales de manera inexacta, incompleta o errada?	**0**
2.	Para los datos almacenados en bases de datos, ¿posee mecanismos técnicos que conserven los datos de carácter personal exactos y actualizados?	**2**
3.	¿Existe un control de los datos personales actualizados en la base de datos?	**2**
4.	¿Se tiene presente que cualquier cambio que se ejecute en los datos personales requiere que se realice en todos los programas o sistemas de la organización que utilizan estos datos?	**2**
Factor: Seguimiento de la información		**Valor**
5.	¿Se realiza algún tipo de seguimiento a la información almacenada en la bases de datos antes de su utilización?	**1**
6.	De los datos personales almacenados en las bases de datos, ¿se lleva un seguimiento que pueda verificar que ésta no sea utilizada para finalidades distintas a las determinadas en la recolección?	**1**
Factor: Redundancia de datos		**Valor**
7.	¿Se presenta con frecuencia datos duplicados en el sistema de información?	**2**
8.	¿Se cancelan inmediatamente datos duplicados en el sistema?	**NAP**
9.	Antes de eliminar datos duplicados se verifica si existe realmente una copia de estos.	**NAP**
10.	¿Es necesaria una autorización para el administrador de la base de datos en caso que desee eliminar un dato duplicado?	**NAP**
Derecho de protección de datos: Datos sensibles		
Factor: Registros de operación de los datos		**Valor**
11.	De los datos sensibles que son almacenados en el sistema de información, ¿se dispone de un registro de operación que permita conocer los procedimientos que se le realizan a los datos?	**2**

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Almacenamiento de datos	
Derecho de protección de datos: Seguridad de datos	
Factor: Medidas técnicas de seguridad	**Valor**
1. En su organización, ¿el administrador de la base de datos ha establecido medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos en sistemas, centros de cómputos, software y hardware, equipos, personas que utilizan y manejan la información almacenada en las bases de datos?	**1**
2. En caso que su organización cuente con estas medidas de seguridad, ¿estas han sido redactadas y documentadas en un documento como políticas o medidas de seguridad para los datos?	**0**
3. ¿En este documento están claramente definidos todas las normas, procedimientos, reglas y estándares, para garantizar un nivel de seguridad que permita la conservación de los datos?	**0**
Factor: Documentación de los sistemas de información	**Valor**
4. ¿Los sistemas de información utilizados para el manejo de datos personales se encuentran debidamente documentados?	**1**
5. ¿En la documentación se especifica el nombre del sistema que se utiliza para el tratamiento de los datos, sus funciones y otros datos referentes como al equipo servidor en el que se encuentra almacenada la base de datos?	**1**
6. ¿La documentación del sistema cuenta con los respectivos diagramas y modelos que se utilizaron para el diseño, estructura de la base de datos, diccionario de datos y la descripción de cada una de las entidades que componen las bases de datos?	**1**
Factor: Estructura de las bases de datos	**Valor**
7. ¿La base de datos dispone de un diseño físico y lógico?	**2**
8. ¿Posee el diccionario de datos un diseño físico y lógico?	**0**
Factor: Cambios en la estructura de las bases de datos	**Valor**
9. ¿Es necesaria la autorización del administrador de la base de datos para realizar cambios a la base de datos?	**NAP**
10. ¿Las modificaciones se realizan sobre una copia de la base de datos?	**NAP**
11. ¿Se realiza un bloqueo sobre la parte de la base de datos a modificar?	**NAP**
12. ¿Se comunica a los diferentes usuarios o desarrolladores del sistema el bloqueo realizado y los posibles fallos de funcionamiento que se pueden presentar?	**NAP**
13. ¿Se realizan pruebas sobre el cambio realizado para verificar que el sistema funciona correctamente?	**NAP**
14. ¿Existen registros o bitácoras en donde se documentan y almacenan todos los cambios realizados a la base de datos, como la petición de cambio, script del cambio realizado, entre otros?	**NAP**
15. ¿Se actualiza el diccionario de datos después del cambio realizado en la base de datos?	**NAP**

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Almacenamiento de datos	
Derecho de protección de datos: Seguridad de datos	
Factor: Registro de incidencias	**Valor**
16. ¿Existe un procedimiento de notificación y gestión de incidencias para la dependencia?	**2**
17. Si la anterior respuesta es positiva, ¿se registra el tipo de incidencia, el momento en que se ha producido, persona que realiza la notificación, persona a quien se le comunica, además de las medidas adoptadas para la solución?	**2**
18. En caso de que exista este registro de incidencia, ¿este contiene el procedimiento de restauración de datos utilizados, los datos restaurados y datos que fueron restaurados manualmente?	**1**
Factor: Gestión de soporte	**Valor**
19. ¿Poseen inventariado y almacenado todos los soportes informáticos que contienen datos de carácter personal?	**1**
20. Existe un registro de autorización y un registro de salida de los soportes informáticos que contienen información de carácter personal hacia otras dependencias de la empresa u otras entidades.	**2**
Factor: Copias de seguridad y recuperación de datos	**Valor**
21. ¿Se realizan copias de seguridad de los datos almacenados en la base de datos?	**2**
22. ¿Existen procedimientos para la realización de copias de seguridad y procedimientos para la restauración del sistema y la recuperación de datos?	**1**
23. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación y restauración de datos garantizan la reconstrucción de estos al estado en el que se encontraban al tiempo de producirse la pérdida o destrucción de la información.	**2**
24. ¿Las copias de seguridad se almacenan en dispositivos externos?	**2**
25. ¿Se verifica que los datos almacenados en soporte externo pueden utilizarse?	**1**
26. ¿El procedimiento para la restauración de los datos, es conocido sólo por los administradores del sistema o de la base de datos?	**2**
27. ¿Los dispositivos externos en donde se almacenan las copias de seguridad se encuentran ubicados en locales diferentes a donde se encuentran los servidores y redes?	**2**

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Almacenamiento de datos	
Derecho de protección de datos: Seguridad de datos	
Factor: Seguridad física de los equipos	**Valor**
28. Existe un inventario con la descripción de los equipos informáticos utilizados para el tratamiento de datos (servidores, terminales, ordenadores, etc.)	**2**
29. ¿En el lugar donde están ubicados los servidores y otros dispositivos que almacenen información personal existe un acceso restringido, solo a personal autorizado?	**2**
30. ¿Hay algún dispositivo o mecanismo de seguridad física (cámaras, alarmas, vigilantes, etc.) en el lugar en donde están ubicados los servidores?	**0**
31. ¿Se poseen dispositivos extras en el caso de caída o que falle el equipo principal?	**2**
32. ¿Se cuentan con un generador de energía auxiliar para suministrar corriente eléctrica a los servidores, en caso de algún fallo en el fluido eléctrico?	**2**

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI

SECCIÓN 3. DETALLES DE LA EVALUACIÓN

Siglas

PCE: Promedio de Cumplimiento Etapa	**PCD:** Promedio de Cumplimiento Derecho	**PCF:** Promedio de Cumplimiento Factor
NCE: Nivel de Cumplimiento Etapa	**NCD:** Nivel de Cumplimiento Derecho	**NCF:** Nivel de Cumplimiento Factor

ETAPA				PCE	NCE
Almacenamiento de datos				**1.58**	**Medio**
Derecho de Protección de Datos	**Factor**	**PCF**	**NCF**	**PCD**	**NCD**
Calidad de datos	Actualización de datos	**1.50**	**Medio**	**1.50**	**Medio**
	Seguimiento de la información	**1.00**	**Medio**		
	Redundancia de datos	**2.00**	**Alto**		
Datos Sensibles	Registro de operaciones de los datos	**2.00**	**Alto**	**2.00**	**Alto**
Seguridad de datos	Medidas técnicas de seguridad	**0.33**	**Bajo**	**1.25**	**Medio**
	Documentación de los sistemas de información	**1.00**	**Medio**		
	Estructura de las bases de datos	**1.00**	**Medio**		
	Cambios en la estructura de las bases de datos	**NAP**	**NAP**		
	Registro de incidencias	**1.66**	**Alto**		
	Gestión de soporte	**1.50**	**Medio**		
	Copias de seguridad y recuperación de datos	**1.71**	**Alto**		
	Seguridad física de los equipos	**1.60**	**Alto**		

Tabla 57. Evaluación del cumplimiento de los derechos de protección de datos en la etapa de utilización de datos

	***M****ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE* ***P****ROTECCIÓN DE* ***D****ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI		
SECCIÓN 1. DETALLES DE LA ORGANIZACIÓN Y DERECHOS A EVALUAR		
Organización:	Universidad del Magdalena	
Área:	Admisiones Registro y Control Académico – ARCA	
Proceso:	Admisión de aspirantes en los programas de pregrado presencial	
Sistema de información:	Sistema de información de ARCA	
Personal evaluado		
Encuestados	**Cargo**	
Ingeniero Álvaro Gamarra	Administrador de servidores	
Ingeniero Wilmer Rueda	Coordinador de control y registro académico	
Ingeniero Jhon Mario Martínez	Coordinador selección de estudiantes	
Evaluadores:		
Ivonne Cabarcas Herrera, Elsy Cantillo Cabarcas, Vanesa Viloria Machado		
Fecha inicio: 8 de julio 2008	**Fecha finalización:**	
Etapa: Utilización de datos		
Derecho de protección de datos	**Factores**	
Datos sensibles	Publicación de datos sensibles (NAP)	
	Soporte informático	
	Acceso a datos sensibles	
Seguridad de datos	Funciones y obligaciones del personal	
	Pruebas con datos personales	
	Planes de contingencia	
Deber de secreto	Compromiso de reserva de información	
	Autorización limitada a las funciones y actividades a desempeñar	
Comunicación de datos o cesión	Certificado de cesión de datos	
	Peticiones de cesión de datos	
	Control de cesión de datos	
Transferencia internacional (NAP)	Control de transferencia de datos	
	Registro de transferencia de información	
	Soportes de la información transferida	
	Convenio de transferencia	
	Políticas de seguridad	
Valoración		
(0): No se cumple	**(1):** No se cumple totalmente	**(2):** Se cumple

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Utilización de datos	
Derecho de protección de datos: Datos sensibles	
Factor: Publicación de datos sensibles	**Valor**
1. Al publicar datos sensibles en páginas Web de su institución, ¿solicita autorización del titular?	**2**
Factor: Soporte informático	**Valor**
2. ¿Se verifica que la salida de soportes informáticos que contienen datos sensibles fuera de la entidad, únicamente podrá ser autorizada por el responsable de los datos en la entidad o en la dependencia?	**2**
3. ¿Se adoptan las medidas necesarias cuando un soporte informático de datos sensibles va a ser desechado o reutilizado de manera que se evite cualquier recuperación de la información almacenada en él previamente?	**NAP**
Factor: Acceso a datos sensibles	**Valor**
4. ¿Se asegura que sólo personal autorizado utiliza y tiene acceso a los datos sensibles, y que están debidamente registrados todos los accesos que se realizan a estos datos a través del sistema?	**2**
5. ¿Se cancelan inmediatamente los derechos de acceso de los usuarios que manejan datos sensibles una vez que cambian de funciones o se desvinculan de la organización?	**2**
Derecho de protección de datos: Seguridad de datos	
Factor: Funciones y obligaciones del personal	**Valor**
1. ¿Existe un manual que define y documenta claramente las funciones y obligaciones del personal, los tipos de accesos y permisos a los sistemas y datos, permitiendo relacionarlos por grupo de usuarios, por perfiles de usuarios o por funciones laborales?	**0**
2. ¿Todos los miembros de la entidad tales como trabajadores, administrativos, directivos y demás empleados; tienen conocimiento de sus funciones y obligaciones y su deber de conservar la seguridad en la información que manejan?	**2**
3. Dentro de las funciones establecidas en la organización, existe personal informático asignado para: administrar redes, administrar sistemas operativos, administrar bases de datos, operadores de bases de datos y para la aplicación de acceso a las bases de datos, personal de mantenimiento de los sistemas y aplicaciones.	**2**

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Utilización de datos	
Derecho de protección de datos: Seguridad de datos	
Factor: Pruebas con datos personales	**Valor**
4. Si es necesario realizar pruebas en el sistema con datos personales ¿Se verifica con anterioridad que el personal encargado tiene la información adecuada y necesaria?	**2**
5. ¿Al momento de realizar pruebas con los datos, el personal encargado tiene un plan de prueba que contenga, una descripción del tipo de prueba a realizar, fecha de inicio de la prueba, los recursos a utilizar en las pruebas como, hardware, humanos, entre otros y la descripción de pruebas realizadas satisfactoriamente?	**0**
6. Si la prueba necesariamente implica tratar datos personales confidenciales ¿se verifica que sean datos no reales, y en el caso que deban ser reales, se asegura que sean eliminados después de finalizada la prueba?	**1**
7. En el caso que la prueba se realice con datos personales confidenciales y reales y no sea posible eliminar los datos ¿se verifica que solo personal autorizado puede realizar las pruebas y que están debidamente registrados todos los accesos que se realizan?	**1**
Factor: Planes de contingencia	**Valor**
8. ¿La organización cuenta con planes de contingencia, que garanticen continuidad y buen funcionamiento en el sistema en caso que ocurra algún imprevisto?	**0**
9. ¿El personal conoce que la organización dispone de planes de contingencia, si ocurre algún inconveniente?	**0**
10. ¿El plan de contingencia identifica todos los posibles riesgos y alternativas o soluciones a los problemas o inconvenientes que se pueden presentar?	**0**
Derecho de protección de datos: Deber de secreto	
Factor: Compromiso de reserva de información	**Valor**
1. ¿Se le informa al administrador de la base datos y a los usuarios del sistema que registran, acceden, procesan y utilizan datos de carácter personal, que están obligados a guardar secreto profesional?	**2**
2. ¿Se supervisa a todo el personal que accede a archivos que contienen datos personales, que cumplan con el compromiso de reservar la información contenida en el sistema de información?	**0**
3. ¿Se ha presentado algún caso donde se infrinja el deber de secreto durante el tratamiento de información de datos personales?	**2**
4. ¿Se le notifica al personal que accede a la base de datos, las consecuencias de incumplimiento de guardar secreto profesional de los datos personales que se almacenan en el sistema de información?	**2**
5. ¿Se sanciona al responsable de la información una vez que incumpla el deber de secreto?	**2**

	***M****ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE* ***P****ROTECCIÓN DE* ***D****ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Utilización de datos	
Derecho de protección de datos: Deber de secreto	
Factor: Autorización limitada a las funciones y actividades a desempeñar	**Valor**
6. ¿El acceso a los datos personales almacenados en las bases de datos, se restringe sólo a personal autorizado, limitado a las funciones y actividades a desempeñar?	**2**
Derecho de protección de datos: Comunicación de datos o cesión	
Factor: Certificado de cesión de datos	**Valor**
1. ¿Cede o comunica datos almacenados en las bases de datos de su organización a terceras personas?	**2**
2. ¿Posee un certificado o documento que compruebe la cesión?	**2**
3. ¿Se verifica que en este documento está claramente determinada la finalidad de la cesión?	**2**
4. Al momento de ceder o recibir datos de otro operador, certifica o pide certificación en donde el titular de la información ha dado su consentimiento para almacenar, procesar y utilizar sus datos.	**0**
5. ¿Se garantiza el correcto uso de los datos de carácter personal durante el tiempo que esté vigente el documento de cesión de acceso a los mismos?	**0**
Factor: Peticiones de cesión de datos	**valor**
6. ¿Se resuelven peticiones del titular de la información para su beneficio?	**2**
7. ¿Se atienden las peticiones de cesión de datos acerca de información registrada en bases de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público?	**2**
Factor: Control de cesión de datos	**Valor**
8. ¿Se le informa al titular de la información de las posibles cesiones a realizar con sus datos?	**0**
9. ¿Se adquiere la autorización del titular de la información para comunicar o ceder sus datos a terceras personas?	**0**
10. Dentro de las instalaciones de la organización, ¿se lleva control de los datos cedidos a terceros que son procesados en el sistema de información?	**2**
11. ¿Existen procedimientos formales para controlar la cesión de datos a través de la red?	**2**

	***M****ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE* ***P****ROTECCIÓN DE* ***D****ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Utilización de datos	
Derecho de protección de datos: Transferencia internacional	
Factor: Control de transferencia de datos	**Valor**
1. ¿Su organización transfiere datos personales almacenados en bases de datos a entidades internacionales o dependencias de gobiernos extranjeros?	**NAP**
2. Al realizar transferencias internacionales de datos ¿se asegura que el destinatario proporcione las garantías adecuadas para el procesamiento de los datos y utilice la información para fines legales y éticos?	**NAP**
3. ¿Se le solicita al responsable de la base de datos o al encargado de la transferencia que aporte documentación complementaria para autorizar dicha transferencia?	**NAP**
Factor: Registro de transferencia de información	**Valor**
4. Al solicitar servicio de alojamiento de datos en un servidor, ¿se asegura que este se encuentra en el lugar donde reside y que dichos datos no son enviados a otro país?	**NAP**
5. ¿Se mantiene un registro histórico de la transferencia de archivos ya efectuados y de las empresas que han participado de ellos, donde se especifique la fecha, datos a transferir, nombre del destinatario, finalidad y país?	**NAP**
6. ¿Se conservan copias de seguridad de los registros que administran la información que es transferida?	**NAP**
Factor: Soporte de la información transferida	**Valor**
7. Se trasladan soportes de la información transferida fuera de las instalaciones sin la autorización necesaria y sin los controles que se hayan establecido.	**NAP**
8. Al momento de transferir datos a otros países ¿Se poseen soportes de la información transferida en la que se pueda verificar el consentimiento del titular del dato?	**NAP**

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI	
SECCIÓN 2. DETALLES DE LA VALORACIÓN	
Etapa: Utilización de datos	
Derecho de protección de datos: Transferencia internacional	
Factor: Convenio de transferencia	**Valor**
9. ¿Existe un convenio con el país o con la entidad extranjera a donde se van transferir los datos personales, de tal manera que este garantice la protección?	**NAP**
10. ¿En el convenio se define algún periodo de eventos (envíos y reenvíos) de los datos que son transferidos a otro país?	**NAP**
11. En el convenio establecido, ¿se le informa al titular de la información que no es necesario solicitar su consentimiento cuando la transferencia sea necesaria para la ejecución o celebración de un contrato, cuando sea necesario proteger el interés público, o sea necesaria la transferencia para la prevención o el diagnóstico médico, entre otros?	**NAP**
12. ¿Se transfiere los datos de carácter personal de sus archivos de clientes, proveedores, trabajadores, entre otros, a su empresa matriz con domicilio fuera del país, por motivos de centralización de información, gestión de recursos, procesos de reorganización?	**NAP**
13. ¿Se definen en el convenio de transferencia acciones a tomar cuando se sospeche de actividades no autorizadas en la transferencia de los datos?	**NAP**
Factor: Políticas de seguridad	**Valor**
14. Antes de transferir datos, ¿se asegura de que el país destinatario brinde y garantice niveles de protección adecuados a dichos datos?	**NAP**
15. ¿Se ejerce vigilancia sobre el destino de los datos que son transferidos?	**NAP**
16. Para la transferencia internacional de datos, ¿se establecen procedimientos para reconocer actividades no autorizadas con la información?	**NAP**
17. ¿Se le proporciona al titular información sobre la finalidad del tratamiento y la identidad del responsable del tratamiento de los datos en el tercer país, así como cualquier otra información en la medida en que sea necesaria para garantizar el tratamiento leal?	**NAP**
18. ¿Su organización efectúa la transferencia internacional solo a petición del titular de la información o de la organización con la que se tiene convenio?	**NAP**

	***M****ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE* ***P****ROTECCIÓN DE* ***D****ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 4. EVALUACIÓN DEL CUMPLIMIENTO DE LOS DPD EN EL SI

SECCIÓN 3. DETALLES DE LA EVALUACIÓN

Siglas

PCE: Promedio de Cumplimiento Etapa	**PCD:** Promedio de Cumplimiento Derecho	**PCF:** Promedio de Cumplimiento Factor
NCE: Nivel de Cumplimiento Etapa	**NCD:** Nivel de Cumplimiento Derecho	**NCF:** Nivel de Cumplimiento Factor

ETAPA	**PCE**	**NCE**
Utilización de datos	**1.48**	**Medio**

Derecho de Protección de Datos	**Factor**	**PCF**	**NCF**	**PCD**	**NCD**
Datos sensibles	Publicación de datos sensibles	**2.00**	**Alto**	**2.00**	**Alto**
	Soporte informático	**2.00**	**Alto**		
	Acceso a datos sensibles	**2.00**	**Alto**		
Seguridad de datos	Funciones y obligaciones del personal	**1.33**	**Medio**	**0.77**	**Bajo**
	Pruebas con datos personales	**1.00**	**Medio**		
	Planes de contingencia	**0.00**	**Bajo**		
Deber de secreto	Compromiso de reserva de información	**1.50**	**Medio**	**1.75**	**Alto**
	Autorización limitada a las funciones y actividades a desempeñar	**2.00**	**Alto**		
Comunicación de datos o cesión	Certificado de cesión de datos	**1.20**	**Medio**	**1.40**	**Medio**
	Peticiones de cesión de datos	**2.00**	**Alto**		
	Control de cesión de datos	**1.00**	**Medio**		
Transferencia internacional	Control de transferencia de datos	**NAP**	**NAP**	**NAP**	**NAP**
	Registro de transferencia de información	**NAP**	**NAP**		
	Soportes de la información transferida	**NAP**	**NAP**		
	Convenio de transferencia	**NAP**	**NAP**		
	Políticas de seguridad	**NAP**	**NAP**		

5.2.4 Analizar y esquematizar la situación del proceso evaluado, según los resultados obtenidos en la evaluación del nivel de cumplimiento y graficar estos resultados

En esta actividad se diligencia el formato para analizar el proceso evaluado (Ver Tablas 58-61) y se grafican los resultados obtenidos.

Tabla 58. Análisis del proceso evaluado en la etapa de recolección y registro de datos

	***M****ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE* ***P****ROTECCIÓN DE* ***D****ATOS EN LOS SISTEMAS DE INFORMACIÓN*
FORMATO Nº 5. ANÁLISIS DE LOS PROCESOS EVALUADOS	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico
Proceso:	Admisión de aspirantes en los programas de pregrado presencial
Sistema de información:	Sistema de información de ARCA
Etapa: Recolección y registro de datos	
ANÁLISIS	**Derecho de protección de datos: Calidad de datos**
	▪ **Factor redundancia de datos.** La dependencia ARCA registra la información recolectada en una sola base de datos. ▪ **Factor control de entradas en campos.** No se requiere previa autorización para ingresar datos en los campos la base de la base de datos. Sin embargo se lleva un control de los datos que se registran en los campos de la base de datos mediante tablas de auditoría en las cuales se verifican los descuentos y exoneraciones. Por otra parte, el diseño de la base de datos no permite dejar campos vacíos cuando se ingresan datos, de lo contrario se activan mensajes de alerta, además este diseño establece el rango máximo y mínimo de caracteres o dígitos. ▪ **Factor seguimiento de la información.** La dependencia ARCA recolecta información a través de aplicaciones Web al iniciar el proceso admisión y luego realiza un seguimiento de la información con documentos físicos, para que los datos sean reales y completos.
	Derecho de protección de datos: Derechos de Información en la Recogida
	▪ **Factor procedimiento de recogida de datos personales.** La dependencia ARCA no le informa a los aspirantes en los programas de pregrado presencial, la creación de una base de datos que almacenará sus datos, la finalidad para que serán tratados, del carácter obligatorio o facultativo de suministrar su datos; sin embargo se le informa del derecho que tiene de acceder, rectificar, cancelar sus datos en la base de datos. La dependencia recoleta los datos directamente del aspirante mediante el formulario de inscripción que se encuentra en la Web. ▪ **Factor documento de soporte.** En el momento de recolectar y registrar datos personales en la base de datos no se solicita autorización por escrito del titular de los datos, ni se le informa de la finalidad de la recogida de los datos. ▪ **Factor finalidad.** Los datos personales almacenados en la base de datos guardan directa relación con la finalidad por la cual se recolectaron.

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 5. ANÁLISIS DE LOS PROCESOS EVALUADOS

Etapa: Recolección y registro de datos

ANÁLISIS

Derecho de protección de datos: Consentimiento

- **Factor autorización del titular del dato.** Para recolectar y registrar datos personales de los admitidos en la base de datos de la dependencia ARCA, no se solicita el consentimiento del aspirante.
- **Factor procedimiento de publicación de datos personales.** La dependencia en este periodo académico optó por no publicar datos personales sin el consentimiento del aspirante, al momento de mostrar los resultados de los admitidos, estos se registraron solamente por carreras y con un número de credencial que identifica a cada uno.

Derecho de protección de datos: Datos Sensible

- **Factor autorización para la administración de datos sensibles.** La dependencia ARCA requiere datos referentes al origen racial y étnico para realizar descuentos en la matrícula de los admitidos, sin embargo se recolectan y registran estos datos sin el consentimiento previo por escrito del titular, además no se le informa que tiene el derecho a no declarar sobre estos datos.

Tabla 59. Análisis del proceso evaluado en la etapa de procesamiento de datos

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 5. ANÁLISIS DE LOS PROCESOS EVALUADOS	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico
Proceso:	Admisión de aspirantes en los programas de pregrado presencial
Sistema de información:	Sistema de Información de ARCA
Etapa: Procesamiento de datos	
ANÁLISIS	**Derecho de protección de datos: Seguridad de Datos**
	▪ **Factor identificación y autenticación.** Las cuentas de usuarios las genera el administrador del sistema y las contraseñas las crea el usuario. Las contraseñas no tienen requisitos de complejidad, solo tienen definida una longitud máxima, y no las cambian periódicamente. Además, no existen procedimientos de bloqueo y desbloqueo por utilización reiterada de contraseñas incorrectas. ▪ **Factor control de acceso.** El administrador de la base de datos gestiona y controla los perfiles de usuarios. En la dependencia ARCA se aplica un control de acceso a los datos y recursos, de acuerdo a sus funciones laborales. Por otra parte, la base de datos cuenta con tablas de auditorías que registran entre otras cosas, los accesos y las acciones que realiza cada usuario. ▪ **Factor restauración de datos.** En el momento de procesar los datos, la dependencia ARCA no cuenta con mecanismos que al reiniciar la ejecución de un proceso interrumpido permitan continuar con el procesamiento de los datos sin repetir o sin dejar de procesar algunas operaciones. Además la restauración de datos se realiza a través de una copia de la base de datos más reciente, por lo tanto no garantiza la recuperación de datos en el estado en que se encontraban al tiempo de producirse un fallo en el sistema. Cabe resaltar que hasta el momento no se ha realizado restauración de datos manualmente.

Tabla 60. Análisis del proceso evaluado en la etapa de almacenamiento de datos

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 5. ANÁLISIS DE LOS PROCESOS EVALUADOS	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico
Proceso:	Admisión de aspirantes en los programas de pregrado presencial
Sistema de información:	Sistema de información de ARCA
Etapa: Almacenamiento de datos	
ANÁLISIS	**Derecho de protección de datos: Calidad de datos**
	▪ **Factor actualización de datos.** Existen mecanismos para conservar los datos personales exactos y actualizados, como copias de seguridad, revisión de documentos, llamadas telefónicas, formularios en páginas Web. Al realizar actualizaciones en la base de datos, quedan registradas en tablas de auditorías. El sistema de información está integrado dentro de la dependencia, por lo tanto cualquier cambio realizado desde un computador se ve reflejado en los demás. ▪ **Factor seguimiento de la información.** La dependencia ARCA verifica la información almacenada en la base de datos antes de su utilización, como es el caso de los descuentos a los aspirantes. ▪ **Factor redundancia de datos.** El sistema de información no presenta redundancia de datos, y al momento de ingresar un dato duplicado, el sistema muestra mensajes de alerta comunicando que el dato ya está registrado en la base de datos.
ISIS	**Derecho de protección de datos: Datos sensibles**
	▪ **Factor registro de operación de los datos.** Los procedimientos que se realizan a los datos personales son registrados en las tablas de auditorías que posee la base de datos.

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 5. ANÁLISIS DE LOS PROCESOS EVALUADOS

Etapa: Almacenamiento de datos

Derecho de protección de datos: Seguridad de datos

ANÁLISIS

- **Factor medidas técnicas de seguridad.** La dependencia de ARCA, no tiene un documento que presente las medidas técnicas para garantizar la seguridad de sus datos, centros de cómputos, software y hardware, equipos, personas que utilizan y manejan información en la base de datos. Sin embargo, la dependencia aplica estas medidas.
- **Factor documentación del sistema.** La documentación del sistema de información no está actualizada.
- **Factor estructura de la base de datos.** La base de datos posee un diseño físico y lógico, pero no tienen un diccionario de datos.
- **Factor registro de incidencias.** En la dependencia ARCA se realizan informes de incidencias, que resaltan aspectos importantes como: el tipo de incidencia, fecha, nombre de la persona que realiza la notificación, persona a quien se le comunica, además de las medidas adoptadas para la solución, como por ejemplo el procedimiento de una restauración de datos.
- **Factor gestión de soporte.** Los soportes informáticos se encuentran almacenados y organizados cronológicamente, pero no existe un inventario de estos. Igualmente se almacenan registros de autorización y de salida de los soportes informáticos que contienen información de carácter personal hacia otras dependencias.
- **Factor copias de seguridad y recuperación de datos.** Se realizan copias de seguridad tres veces al día, en un equipo remoto y en el servidor, las cuales solo son almacenadas en estos equipos y en CDs, luego son entregadas al jefe de la dependencia. Por otra parte el procedimiento para la restauración de los datos solo es conocido por el administrador de la base de datos.
- **Factor seguridad física de los equipos.** Se tienen un inventario de los equipos informáticos de la dependencia, que es realizado por la dependencia de ALMACEN. Por otro lado, la dependencia ARCA establece un acceso restringido a personal no autorizado, en el lugar donde se encuentran los servidores y otros dispositivos que almacenan información personal. Esta dependencia no tiene mecanismos de seguridad física, como cámaras, extintores, ente otros, sin embargo, tienen un servidor de respaldo en caso de caída o falla del sistema. Cabe anotar que, solo el servidor tiene un generador de energía auxiliar (UPS), mientras que los equipos locales no tienen regulador.

Tabla 61. Análisis del proceso evaluado en la etapa de utilización de datos

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

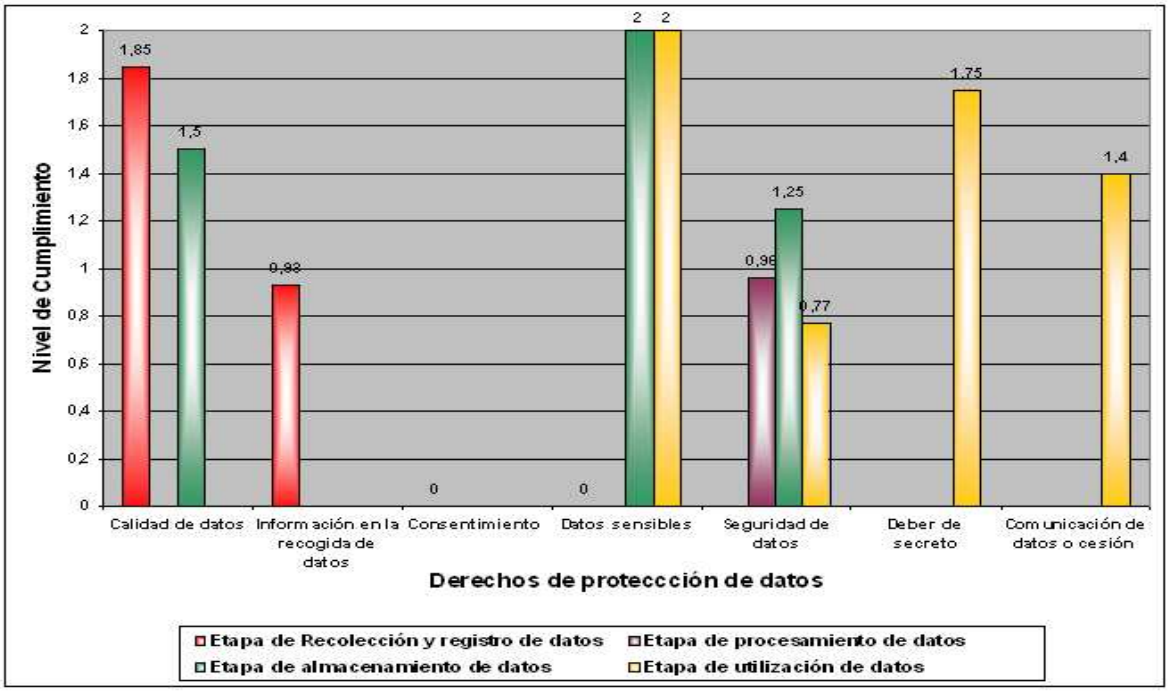
FORMATO Nº 5. ANÁLISIS DE LOS PROCESOS EVALUADOS	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico
Proceso:	Admisión de aspirantes en los programas de pregrado presencial
Sistema de información:	Sistema de información de ARCA
Etapa: Utilización de datos	
ANÁLISIS	**Derecho de protección de datos: Datos sensibles**
	▪ **Factor publicación de datos sensibles.** La dependencia no publica datos sensibles en páginas Web de su institución. ▪ **Factor soporte informático.** La salida de soportes informáticos que contienen datos sensibles a otra dependencia, solo puede ser autorizada por el jefe de la dependencia. ▪ **Factor acceso a datos sensibles.** Solo personal autorizado utiliza y tiene acceso a los datos sensibles, los cuales son registrados en tablas de auditorias. Además, cuando un usuario cambia de funciones en la dependencia se modifican sus derechos de acceso según el rol que desempeñará, y el usuario que es desvinculado de la dependencia se le elimina su cuenta de usuario del sistema.
	Derecho de protección de datos: Seguridad de datos
	▪ **Factor funciones y obligaciones del personal.** La dependencia ARCA no posee un manual de funciones, sin embargo todo el personal conoce sus funciones y obligaciones. Hay personas establecidas para administrar redes, sistemas operativos y base de datos, operar la aplicación de acceso a las bases de datos y personal de mantenimiento de los sistemas y aplicaciones. ▪ **Factor pruebas con datos personales.** Cuando la dependencia ARCA realiza pruebas con datos personales en el sistema, se utilizan copias de seguridad recientes, por lo tanto se tiene la información real y necesaria, pero no se crea un registro que muestre los detalles de la prueba a realizar. ▪ **Factor planes de contingencia.** La dependencia ARCA no dispone de planes de contingencia.
	Derecho de protección de datos: Deber de secreto
	▪ **Factor compromiso de reserva de información.** El jefe de la dependencia ARCA, comunica a los usuarios que tiene acceso a datos personales, el compromiso de reservar información, pero no se supervisa el cumplimiento de este compromiso. Hasta el momento, no se han presentado casos de incumplimiento, pero existen sanciones para ello. ▪ **Factor autorización limitada a las funciones y actividades a desempeñar.** En la dependencia ARCA se restringe el acceso a los datos de carácter personal almacenados en registros o archivos en el sistema de información a personal autorizado, de acuerdo a las funciones y actividades que desempeñan.

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 5. ANÁLISIS DE LOS PROCESOS EVALUADOS	
Etapa: Utilización de datos	
ANÁLISIS	**Derecho de protección de datos: Comunicación de datos o Cesión**
	▪ **Factor certificado de cesión de datos.** Cuando una dependencia solicita información de carácter personal a la dependencia ARCA, esta verifica que el documento de solicitud tenga definida la finalidad por la cual requiere dicha información, y al momento de cederla se registra un certificado de cesión de datos, pero no se tiene en cuenta la autorización del titular de los datos, en este caso son los aspirantes en los programas de pregrado presencial a la Universidad del Magdalena, para ceder sus datos a otras dependencias. ▪ **Factor petición de cesión de datos.** La dependencia resuelve en lo posible peticiones de los aspirantes en los programas de pregrado presencial, para su beneficio. Además, atiende peticiones de cesión de datos acerca de información registrada en bases de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público. ▪ **Factor control de cesión de datos.** Cuando la dependencia ARCA cede información a través de la red, aplican procedimientos formales como es la utilización de los correos institucionales, que serán certificaciones para posibles auditorías. Sin embargo, esta dependencia no requiere de la autorización del titular de información para ceder sus datos a terceras personas.

La Figura 21 ilustra el nivel de cumplimiento de los derechos de protección de datos, en cada una de las etapas del procesamiento de datos (recolección y registro, procesamiento, almacenamiento y utilización) del sistema de información de ARCA, el cual es el sistema que sirve de apoyo al proceso de Admisión de estudiantes en los programas de pregrado presencial.

Figura 21. Gráfica del nivel de cumplimiento de los derechos de protección de datos por etapas



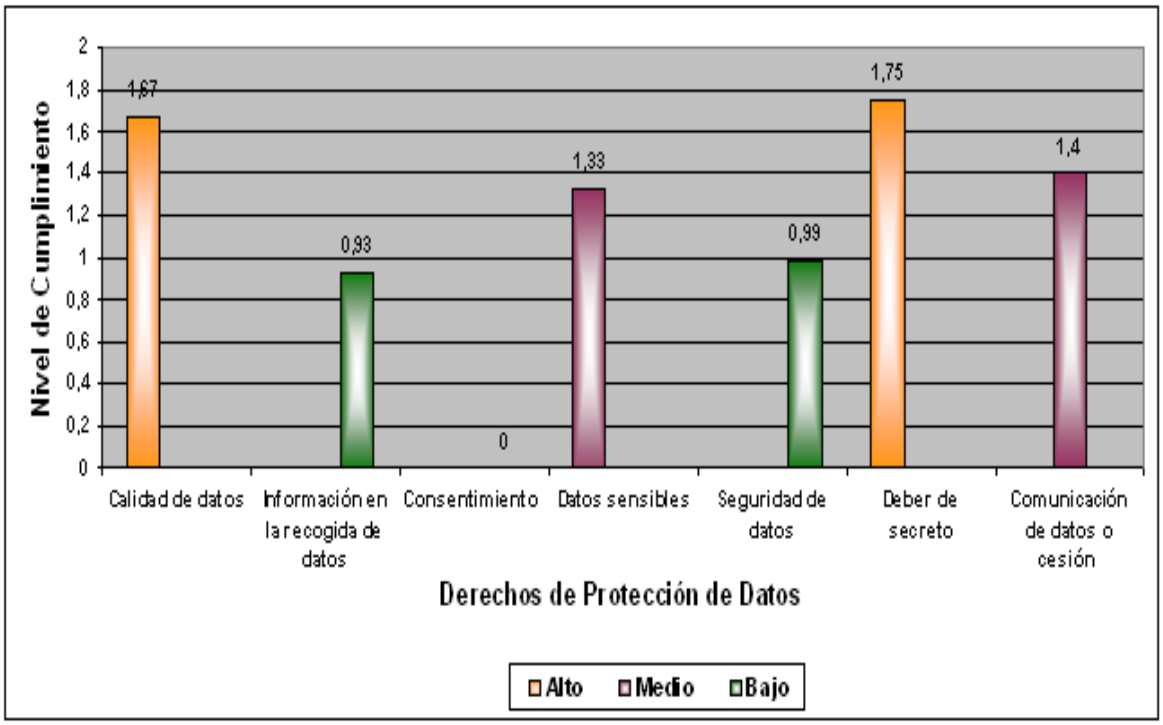
En el capítulo 4, se describió la relación de las etapa del procesamiento de los datos y cada uno de los derechos de protección de datos a evaluar en ella, y se llegó a la conclusión que un derecho de protección de datos puede ser evaluado en una o varias etapas del procesamiento de datos, como muestra la gráfica anterior; sin embargo, para dar un resultado final, la Tabla 62 presenta el nivel de cumplimiento general de cada uno de los derechos de protección de datos, en el sistema de información de ARCA; así mismo, estos resultados son presentados en la Figura 22.

Tabla 62. Resumen del nivel de cumplimiento de los derechos de protección de datos

Derecho de protección de datos	Etapa que evalúa el derecho	Promedio	Promedio total/Nivel de cumplimiento
Calidad de datos	Recolección y registro de datos	1.85	**1.67 / ALTO**
	Almacenamiento de datos	1.50	
Información en la recogida de datos	Recolección y registro de datos	0.93	**0.93 / BAJO**

Derecho de protección de datos	Etapa que evalúa el derecho	Promedio	Promedio total/Nivel de cumplimiento
Consentimiento	Recolección y registro de datos	0.00	**0.00 / BAJO**
Datos sensibles	Recolección y registro de datos	0.00	**1.33 / MEDIO**
	Almacenamiento de datos	2.00	
	Utilización de datos	2.00	
Seguridad de datos	Procesamiento de datos	0.96	**0.99 / BAJO**
	Almacenamiento de datos	1.25	
	Utilización de datos	0.77	
Deber de secreto	Utilización de datos	1.75	**1.75 / ALTO**
Comunicación de datos o Cesión	Utilización de datos	1.40	**1.40 / MEDIO**

Figura 22. Gráfica de niveles de los derechos de protección de datos.



5.2.5 Formular el estado y las recomendaciones del proceso organizacional seleccionado y su sistema de información con respecto al cumplimiento de los derechos de protección de datos

Teniendo en cuenta la evaluación y el análisis realizado anteriormente se procede a formular el estado del proceso de “admisión de aspirantes en los programas de pregrado presencial” por las etapas de procesamiento de datos con respecto al cumplimiento de los derechos de protección de datos:

- El derecho de calidad de datos que se evalúa en las etapas de recolección y registro de datos y de almacenamiento de datos, se encuentra en un nivel de cumplimiento alto, ya que se le realiza un seguimiento a la información personal de los aspirantes, con el fin de almacenar datos exactos, completos y actualizados. Además no se presenta redundancia de datos debido al diseño de la base de datos.

- El derecho de Información en la recogida de datos presenta un nivel de cumplimiento bajo, porque no se le informa al titular de los datos, que en este caso son los aspirantes en los programas de pregrado presencial, de la creación de una base de datos que contendrá sus datos personales y la finalidad para que serán tratados.

- En la etapa de recolección y registro de datos se evalúa el derecho de consentimiento que se encuentra en un nivel de cumplimiento bajo, ya que la dependencia Arca no solicita por escrito la autorización del titular de los datos, para el tratamiento de sus datos personales.

- El derecho de datos sensibles que se evalúa en las etapas de recolección y registro de datos, almacenamiento y utilización de datos, se encuentra en un nivel de cumplimiento medio, porque al utilizar datos referentes al origen racial y étnico en los descuentos de la matrícula de los admitidos, estos solos son

accesados por personal autorizado y se registran cada uno de estos accesos, además no son publicados o dados a conocer a terceras personas sin una previa autorización o control.

- En las etapas de procesamiento, almacenamiento y utilización de datos, se evalúa el derecho de seguridad de datos, que presenta un nivel de cumplimiento bajo, porque no adoptan suficientes medidas técnicas y organizativas para garantizar la seguridad de los datos personales, como por ejemplo, no tiene mecanismos de seguridad física (cámaras, extintores); no tienen planes de contingencias; no poseen un manual de funciones, sin embargo todo el personal conoce sus funciones y obligaciones, los procedimientos establecidos para la recuperación y restauración de datos no garantizan la reconstrucción de estos en el momento en el que se encontraban al tiempo de producirse un fallo en el sistema; no existen procedimientos de bloqueo y desbloqueo por utilización reiterada de cuentas incorrectas. El sistema de información no tiene una documentación actualizada. Además, las contraseñas poseen un nivel de seguridad bajo y no las cambian periódicamente.

- El derecho de deber de secreto que se evalúa en la etapa de utilización se encuentra en un nivel de cumplimiento alto, ya que se restringe el acceso a datos personales de acuerdo a las funciones a desempeñar en la dependencia, se les comunica el compromiso de reserva de información y se sanciona a las personas que infrinjan el secreto profesional.

- En la etapa de utilización se evalúa el derecho de comunicación de datos o cesión que se encuentra en un nivel de cumplimiento medio, porque ceden información a terceras personas sin previo consentimiento del titular de los datos, sin embargo la dependencia ARCA posee documentos de autorización que muestran la finalidad por la cual el solicitante requiere la información y aplica procedimientos formales para controlar la cesión de datos a través de la red.

Después de conocer el estado con respecto al cumplimiento de los derechos de protección de datos en el sistema de información de ARCA, el cual sirve de apoyo al proceso de admisión de estudiantes en los programas de pregrado presencial, se continúa con el planteamiento de las recomendaciones, a partir de las falencias encontradas y teniendo en cuenta los niveles de seguridad que reglamentan las leyes de protección de datos. (Ver Tablas 63-66).

Tabla 63. Recomendaciones para la etapa de recolección y registro de datos

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*
FORMATO Nº 6. RECOMENDACIONES	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico
Proceso:	Admisión de estudiantes en los programas de pregrado presencial
Sistema de información:	Sistema de información de ARCA
Fecha:	21 de Julio de 2008
Etapa: Recolección y registro de datos	
Derecho de protección de datos: Calidad de datos	
Factor	**Sugerencias**
Control de entradas en campos	Llevar a cabo un control de procesamiento duplicado, que consiste en tener una pre-numeración de formatos para el ingreso de datos o registros de transacciones, ayudando con esto, a que no exista un mismo código para diferentes registros y el sistema controle el cumplimiento de la secuencia de los formatos pre-enumerados.
Derecho de protección de datos: Información en la recogida de datos	
Factor	**Sugerencias**
Procedimiento de recogida de datos personales	Al recolectar datos personales, mediante el aplicativo Web de inscripción, se debe crear una cláusula o un término legal en donde se le informe a los aspirantes de forma precisa y comprensible de la creación de una base de datos que almacenará sus datos personales; de la finalidad de la recogida de los datos y de los destinatarios de la información; del carácter obligatorio o facultativo de suministrar los datos que le sean solicitados, y las consecuencias de proporcionar datos no exactos o falsos; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación de los datos y oposición de los datos que serán almacenados en bases de datos. Cabe anotar que esta cláusula debe aparecer antes de registrar los datos personales de los aspirantes.

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*

FORMATO Nº 6. RECOMENDACIONES	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico
Proceso:	Admisión de estudiantes en los programas de pregrado presencial
Sistema de información:	Sistema de información de ARCA
Fecha:	21 de Julio de 2008

Etapa: Recolección y registro de datos	
Derecho de protección de datos: Información en la recogida de datos	
Factor	**Sugerencias**
Documento de soporte	El aplicativo Web debe generar un documento que debe ser impreso y firmado por el aspirante para certificar que éste desea voluntariamente proporcionar sus datos personales, y luego entregarlo a la dependencia junto con los demás documentos.
Derecho de protección de datos: Consentimiento	
Factor	**Sugerencias**
Autorización del titular del dato	Además de informar a los aspirantes a través de la cláusula anteriormente mencionada, el aplicativo Web debe tener una opción de aceptar o no, el consentimiento del aspirante para el tratamiento de sus datos personales.
Procedimiento de publicación de datos personales	Antes de publicar datos personales que son de interés para los aspirantes, se debe tener un mecanismo para comunicar y obtener una certificación por escrito de su consentimiento; el cual puede ser a través de correos electrónicos, llamadas telefónicas o mensajería.
Derecho de protección de datos: Datos sensibles	
Factor	**Sugerencias**
Autorización para la administración de datos sensibles	La cláusula mencionada anteriormente, debe tener una opción que indique si el aspirante pertenece a comunidades indígenas, es desplazado, afrocolombiano, mujer cabeza de familia, entre otros datos sensibles, para que genere un documento (en caso que si lo sea) certificando el consentimiento de proporcionar sus datos personales para que sean tratados, el cual se pueda imprimir, para que sea firmado por el aspirante y luego entregado a la dependencia junto con los demás documentos. Cabe anotar que este documento es diferente al que se menciona en el factor documento de soporte del derecho de protección de datos “información en la recogida de datos”.

Tabla 64. Recomendaciones para la etapa de procesamiento de datos

	***M**ODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE **P**ROTECCIÓN DE **D**ATOS EN LOS SISTEMAS DE INFORMACIÓN*
FORMATO Nº 6. RECOMENDACIONES	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico
Proceso:	Admisión de estudiantes en los programas de pregrado presencial
Sistema de información:	Sistema de información de ARCA
Fecha:	21 de Julio de 2008
Etapa: Procesamiento de datos	
Derecho de protección de datos: Seguridad	
Factor	**Sugerencias**
Identificación y autenticación	Teniendo en cuenta que la autenticación de acceso al sistema de información de ARCA se realiza por medio de contraseñas, se deben fijar ciertas normas para mantener seguros los datos: · Fijar la duración máxima de vigencia de la contraseña · Definir requisitos de complejidad (números y letras), · Establecer los procedimientos de generación, asignación, conservación y almacenamiento seguro de contraseñas · Establecer procedimientos de bloqueo y desbloqueo de cuenta por utilización reiterada de contraseñas incorrectas.
Restauración de datos	El sistema de ARCA no cuenta con procedimientos de continuidad y recuperación de datos, se recomienda que al procesar datos, los sistemas cuenten con procedimientos de continuidad, que permitan reiniciar la ejecución de un proceso que por algún motivo fue interrumpido y seguir con la ejecución del mismo, sin repetir operaciones o sin dejar de procesar algunas. Al igual que crear e implementar procedimientos que permitan garantizar la reconstrucción de los datos al estado en que se encontraba al tiempo de producirse el fallo; estos procedimientos son muy importantes para lo sistemas y su ventaja ante los backup radica en que estos sólo reconstruyen los datos almacenados por la copia de seguridad, pero no las últimas operaciones realizadas en el mismo instante en que se presentó el fallo en el sistema, como si lo hacen los procedimientos de continuidad y restauración de datos.

Tabla 65. Recomendaciones para la etapa de almacenamiento de datos

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*
FORMATO Nº 6. RECOMENDACIONES	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico
Proceso:	Admisión de estudiantes en los programas de pregrado presencial
Sistema de información:	Sistema de información de ARCA
Fecha:	22 de Julio de 2008
Etapa: Almacenamiento de datos	
Derecho de protección de datos: Calidad de datos	
Factor	**Sugerencias**
Actualización de datos	En las bases de datos de una organización no se deben manejar datos desactualizados o incorrectos, cuando se conozca que los datos registrados no correspondan con los verdaderos estos deben ser actualizados, así mismo, deben de existir mecanismos técnicos que conserven los datos personales exactos, y tener en cuenta que cuando un dato es cambiado, este cambio debe reflejarse en las bases de datos o consultas realizadas por otro personal dentro del área u otras dependencias.
Seguimiento de la información	Mediante procedimientos debe verificarse que la información a utilizar sea la adecuada y que no se utilice para finalidades distintas.
Derecho de protección de datos: Seguridad	
Factor	**Sugerencias**
Medidas técnicas de seguridad	Se recomienda a la dependencia de ARCA que las medidas de seguridad establecidas y las que debe adoptar, deben ser documentadas como políticas de seguridad, donde se definen una serie de controles, procedimientos y acciones a realizar ante incidencias que pueden ocurrir sobre los sistemas de información; este documento debe mantenerse actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Además, este documento de seguridad es necesario desde el punto de vista práctico, porque permite evaluar históricamente la evolución de los riesgos que afectan los sistemas de información y tomar las mejores decisiones al respecto. En el Anexo A los desarrolladores del proyecto en base al real decreto 994/1999[59] (Ver Anexo B) han diseñado un resumen de lo que puede contener y la organización del documento de seguridad, la creación de éste dentro de la dependencia es responsabilidad del administrador del sistema de información.
Documentación de los sistemas	Se recomienda que la dependencia de ARCA documente el sistema de información utilizado para el manejo de sus datos y actualizarlo cada vez

[59] Por el que se aprueba el Reglamento de Medidas de Seguridad para los Ficheros automatizados de Datos de Carácter Personal para el país de España, el cual establece las medidas de carácter técnico y organizativo que deben ser adoptadas por todas las Empresas, Organizaciones, Asociaciones e Instituciones, tanto Públicas como Privadas, que almacenen, traten y accedan a ficheros de datos de carácter personal.

de información	que se realicen cambios al sistema o se creen nuevas aplicaciones para llevar a cabo sus actividades, esta documentación incluye nombre de quien diseña la aplicación, fecha en que se programó, funciones de cada módulo o aplicación, así mismo se debe anexar todas las características del diseño, como los respectivos diagramas y modelos que se utilizaron para el diseño, además contener las características del sistema operativo, de los controles de acceso y los perfiles, el entorno de sistema operativo y de comunicaciones. Esta documentación puede estar como anexo al documento de seguridad descrito en la recomendación anterior.
Estructura de la bases de datos	Se recomienda documentar la estructura de la base de datos, describir cada una de las entidades que la componen y relación entre las mismas, documentar el diccionario de datos, definir el gestor de base de datos y mecanismos de recuperación, entre otros.
Registro de incidencias	Se recomienda a la dependencia que continué con el procedimiento de registrar los fallos ocurridos, sin embargo sugiere incluir la forma en que son restaurados los datos.
Gestión de soporte	Se consideran como soportes documentos, cartas, informes, volantes, comprobantes, entre otros, y como soportes informáticos los cd's, dispositivos USB, diskette, discos duros, computadores portátiles y demás dispositivos móviles que puedan contener datos personales. La dependencia de ARCA debe de inventariar, rotular y almacenar los soportes informáticos que contienen datos personales, en un lugar de acceso restringido y continuar con los procedimientos de autorización y registro por parte del director para la entrada y salida de los soportes que contienen información personal (Ver Anexo A).
Copias de seguridad y recuperación de datos	Aunque la dependencia realiza backup diarios, se aconseja que este procedimiento sea documentado, al igual que documentar el procedimiento de restauración de datos, el cual debe garantizar la reconstrucción de los datos, los archivos, documentos y bases de datos al momento de producirse la pérdida; estas copias de seguridad y una copia de del procedimiento de restauración de datos se deben almacenar y conservar en un lugar de acceso restringido. Por otro lado, aunque la probabilidad de un desastre natural en las instalaciones de la universidad o de la dependencia de ARCA sea baja, se recomienda almacenar estas copias de seguridad, el procedimiento de restauración, los programas y aplicaciones del sistema, en un lugar diferente a donde normalmente opera.
Seguridad física de los equipos	En el lugar donde están ubicados los servidores y otros dispositivos que almacenen datos, debe protegerse de tal manera que se garantice la disponibilidad y confiabilidad de los datos protegidos. También se debe tener en cuenta que los locales deben ser adecuados para los equipos de cómputo y de contar con acceso restringido solo a personal autorizado.

Tabla 66. Recomendaciones para la etapa de utilización de datos

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*
FORMATO Nº 6. RECOMENDACIONES	
Organización:	Universidad del Magdalena
Área:	Admisiones Registro y Control Académico
Proceso:	Admisión de estudiantes en los programas de pregrado presencial
Sistema de información:	Sistema de información de ARCA
Fecha:	22 de Julio de 2008
Etapa: Utilización de datos	
Derecho de protección de datos: Seguridad de datos	
Factor	**Sugerencias**
Funciones y obligaciones del personal	Formalmente no hay un manual que defina claramente las funciones y obligaciones del personal dentro de la dependencia, se debe tener en cuenta que este manual es muy importante para la organización de esta, se recomienda que sean documentadas todas las funciones y obligaciones del personal con acceso a los datos y a los sistemas de información, en esta documentación se definen los privilegios de acceso y determinar qué usuarios pueden o no acceder a ciertos módulos del sistema y cuales pueden crear, actualizar, modificar o eliminar datos, además se debe comunicar, explicar y capacitar al personal en cuanto a sus funciones, igualmente debe aplicar y realizar un seguimiento del manual de tal manera que las funciones establecidas sean las adecuadas al personal asignado (Ver Anexo A).
Pruebas con datos personales	Al realizar pruebas con datos personales, se recomienda seleccionar un conjunto de datos que contengan información adecuada y precisa para realizar la prueba, además se debe realizar una especie de plan en donde se especifica la descripción del tipo de prueba a realizar, la fecha de inicio y los recursos a utilizar en esta. Cabe resaltar, que el artículo 22 del Reglamento de Medidas de Seguridad[60] establece que no beben utilizarse datos reales; pero, en caso de que se utilicen, deberán adoptarse un buen nivel de seguridad para los datos (Ver Anexos A y B).
Planes de contingencia	La dependencia debe disponer de planes de contingencia que identifiquen todos los posibles riesgos y amenazas, ya sean internas o externas, como incendios, desastres naturales, falla de energía, daños causados por el hombre, errores y omisiones, y definir las alternativas de solución a estos problemas o inconvenientes; los riesgos y controles identificados deben ser formalizados en un documento, en donde se prevean claramente la reacción a emergencia, el plan de respaldo y el plan de acción o recuperación.

[60] Establece que las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

	*MODELO PARA ESTUDIAR Y EVALUAR EL CUMPLIMIENTO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INFORMACIÓN*
FORMATO Nº 6. RECOMENDACIONES	
Etapa: Utilización de datos	
Derecho de protección de datos: Deber de secreto	
Factor	**Sugerencias**
Compromiso de reserva de información	Se debe informar y supervisar al personal que tiene acceso a datos personales sobre la obligación que contrae con la dependencia de no revelar información a personas ajenas a esta.
Derecho de protección de datos: Comunicación de datos o cesión	
Factor	**Sugerencias**
Certificado de cesión de datos	Se recomienda que cada certificado de cesión de datos sea analizado de forma específica de acuerdo con los preceptos legales que establece la ley, para evitar el tratamiento indiscriminado de los datos personales, por lo que es importante que este tipo de certificado de cesión responda a una finalidad concreta, determinada y necesaria.
Control de cesión de datos	Recuerde que si su organización decide ceder datos personales a terceros deberá recabar previamente la autorización del interesado e informarle sobre la posible cesión. Por último tenga en cuenta que al ceder datos está obligado a cumplir con lo dispuesto por la ley (Ver Anexo A).

5.2.6 Monitorear y llevar a cabo acción control

En el transcurso de la aplicación del modelo, se verificó que cada actividad se lleva a cabo de la mejor manera posible, sin embargo se requirió aplicar nuevamente algunas actividades para obtener la información necesaria, que permitió una adecuada evaluación del nivel de cumplimiento de los derechos de protección de datos en el proceso seleccionado, de esta manera se facilitó el planteamiento de sugerencias para mejorar el cumplimiento de estos.

6 CONCLUSIÓN

En primera instancia, se decidió elaborar este proyecto en base a conocimientos adquiridos en la electiva profesional “Auditoría de Sistemas”, a pesar de no ser una de las líneas que comúnmente se utiliza en los proyectos de pregrado en el programa de ingeniería de sistemas de la Universidad de Magdalena, como lo son, ingeniería de software y redes y telecomunicaciones; por ende, al momento de entregar el anteproyecto, se tuvo incertidumbre por la aceptación de este, ya que es un nuevo tema. Después de su aprobación, se empezó a crear su estructura y documentación, para ello se adquirió conocimientos en el área legislativa mediante el estudio de las leyes de protección de datos a nivel nacional e internacional, esto permitió determinar los derechos de protección evaluados por el modelo. Es aquí donde se notó la gran importancia de proteger los datos personales en los sistemas de información de las organizaciones, aunque actualmente en nuestro país hay una ley de protección de datos que se encuentra en espera de aprobación de parte de la Corte Constitucional, caso contrario de los países de España y Argentina que son líderes en el tema.

Igualmente, se hizo necesario el estudio de una nueva metodología que permitiera recoger la complejidad de la situación y realizar de forma iterativa el proceso de definición de los elementos de evaluación antes de ejecutarla en un sistema de información; con la aplicación de esta metodología se obtuvo una experiencia agradable y didáctica que facilitó en gran manera el diseño del modelo, además ayuda a comprender de forma más amplia el impacto de los sistemas de información en las organizaciones humanas; asimismo se logró ampliar los conocimientos en administración de sistemas de información y base de datos, ya que fue necesario tenerlos en cuenta para el buen diseño del modelo.

Una de las dificultadas presentadas a lo largo del desarrollo del proyecto fue la definición, organización y forma de evaluación del modelo, inicialmente el modelo evaluaría solo a los sistemas de información de una organización en forma general; pero de esta manera no se evaluarían todos los aspectos que intervienen en el tratamiento de los datos y no se lograrían los resultados esperados; por tal motivo, fue necesario detallar la evaluación, y se determinó evaluar los procesos que tienen apoyo de sistemas de información y utilizan datos personales; no obstante, después de analizar los procesos de una organización y el procedimiento que se realiza a la información dentro de un proceso, se consideró que en todo procesamiento de datos se distinguen ciertas etapas por las que todo dato debe pasar (recolección y registro de datos, procesamiento, almacenamiento y utilización de datos) y se llegó a la conclusión que estos podrían ser evaluados por estas etapas.

Partiendo de la definición de cada derecho de protección de datos, inicialmente se realizó una serie de interrogantes relacionados con cada uno de estos, sin embargo al avanzar en el desarrollo del modelo, se notó que los derechos comprenden varios temas, como es el de seguridad de datos que incluye la seguridad en los sistemas de información, en el acceso físico a los centros de cómputo, en el personal que accede a los datos y copias de seguridad entre otras cosas; debido a esto surgió la necesidad de organizar y agrupar por factores los interrogantes de los derechos, de acuerdo a las características definidas en cada uno de estos, para facilitar la futura evaluación.

En resumen el modelo está conformado por tres componentes los cuales son, las etapas de procesamiento de datos, derechos de protección de datos relacionados con las etapas y los factores que influyen en los derechos de protección de datos, el modelo se organizó de esta manera para lograr los resultados que inicialmente se esperaban y cumplir con el objetivo propuesto: *garantizar el derecho de habeas data al titular de los datos*.

Después de definir la manera como el modelo evalúa los derechos de protección de datos, se determinaron los mecanismos de recolección de información a utilizar en cada interrogante, y se creó una guía para utilizar estos mecanismos; así mismo se crearon los formatos en donde se registra y analiza la información recolectada.

En la aplicación, se experimentó la necesidad de establecer requerimientos específicos en la recolección y registro, procesamiento, almacenamiento y utilización de datos personales para protegerlos, y hubo la necesidad de replantear algunos factores e interrogantes a evaluar, de esta manera se perfeccionó el modelo diseñado. Además, se detectaron debilidades en el proceso evaluado, y debido a esto se plantearon algunas sugerencias que al ser aplicadas por la dependencia de Admisiones, Registro y Control Académico, garantizará el derecho de habeas data en el proceso de *Admisiones de aspirantes en los programas de pregrado presencial*.

Una de las cosas que se aprendió en la elaboración del documento final, es que siempre se debe redactar para personas que no conozcan el tema, de tal manera que cualquier persona pueda comprender el documento, por ello se debe “escribir no para nosotros, sino para los demás”. Por otra parte, es importante resaltar que este proyecto no finaliza aquí, ya que a partir de lo realizado en este, se puede desarrollar una herramienta software que facilite la realización de auditorías en los sistemas de información, el cual es un aporte a la informática jurídica y a la disciplina sistema de información.

A través de este proyecto, la perspectiva del rol que puede desempeñar un ingeniero de sistemas cambio, se notó que la ingeniería de sistemas no solo comprende temas tecnológicos y aspectos tales como software y hardware, también contempla la administración de sistemas, auditorías de sistemas,

derecho informático, entre otros, y un ejemplo claro de lo anterior es este proyecto, que crea un modelo a partir de conocimientos tecnológicos, técnicos y legislativos, para realizar auditorías en un sistema de información; de esta forma se fortalece un nuevo perfil administrativo para el ingeniero de sistemas.

Finalmente, la experiencia adquirida al realizar este proyecto, es gratificante, por cumplir los objetivos planteados y por comprender el impacto que ha tenido la tecnología de información en la sociedad, por una parte contribuye al progreso social, pero por otra parte amenaza la privacidad de las personas al hacerla rentable y de fácil acceso para copiar y/o manipular información personal. Por ello se crea este proyecto, en el cual se percibe que una parte de esta sociedad está tomando conciencia de la realidad que lo rodea, pero no basta con solo tener conocimiento de esta problemática, es relevante actuar ante estas circunstancias, pero sobre todo, se espera que cada día incremente el número de personas que se apropien de la responsabilidad de proteger los datos personales en los sistemas de información de las organizaciones, y así, poco a poco se irá formando una mejor calidad de vida, en Santa Marta y pronto en Colombia.

BIBLIOGRAFÍA

[1] LAUDON C, Kenneth y LAUDON P, Jane. Sistemas de información gerencial: Organización y tecnología de la empresa conectada en red. 6ª edición. México: Pearson Educación. 2002

[2] REMOLINA ANGARITA, Nelson. Estados Unidos compró base de datos del Registro Nacional de Colombia. En el Tiempo, Bogotá (12, mayo, 2003) p. 1, 2 y 3.

[3] REMOLINA ANGARITA, Nelson. Censos, estadísticas y tratamiento de datos personales en el contexto del gobierno electrónico. En Revista de Derecho, comunicaciones y nuevas tecnologías del GECTI, No 1, p. 207-246. Bogotá: Universidad de los Andes, 2005.

[4] BURCH, John. GRUDNITSKI, Gary. Diseño de sistemas de información: Teoría y práctica. 5ª edición. México D.F: Editorial Limusa. Noriega editores. 2001.

[5] WILSON, Brian. Sistemas: conceptos, metodología y aplicaciones. 1ª edición. México D.F: Editorial Limusa. Noriega editores. 1993.

[6] LAUDON C, Kenneth y LAUDON P, Jane. Sistemas de información gerencial: Organización y tecnología de la empresa conectada en red. 8ª edición. México: Pearson Educación. 2004.

[7] ECHENIQUE G. José. Auditoria informática. Editorial McGraw Hill. 2ª edición. México 2001.

[8] PIATTINI, Mario. Auditoría Informática – Un enfoque practico 2ª Edición. México. Alfa Omega. 2001.

[9] TÉLLEZ VALDES, Julio. Derecho Informático. México. Universidad Nacional Autónoma de México. 1991.

[10] REMOLINA ANGARITA, Nelson. Data protection. Panorama nacional e internacional. EN: Internet Comercio Electrónico & Telecomunicaciones. Colombia: Legis. 2002.

[11] SAGÜES, Néstor, Subtipos de habeas data, J.A., 20 de diciembre de 1995.

[12] CHECKLAND, Peter. SCHOLES, Jim. La metodología de sistemas suaves en acción. 1ª edición. México D.F: Editorial Limusa. Noriega editores. 1994.

[13] KENDALL, Kenneth y KENDALL, Julie. Análisis y diseño de sistemas. 3ª edición. México D.F. Editorial Pearson Educación. 1997.

[14] SENN, James A. Sistemas de información para la administración. 3ª Edición. México, D.F. Editorial Grupo editorial Iberoamerica. 1990.

[15] REMOLINA ANGARITA, Nelson. Centrales de información, hábeas data y protección de datos personales: avances, retos y elementos para su regulación. EN: Derecho de Internet & Telecomunicaciones. Colombia. Legis. 2003

[16] Congreso de la República de Colombia. Ley 221/07 Derechos de habeas data en Colombia. Santa fe de Bogota. Ley en proceso de aprobación por parte de la Corte Constitucional.

[17] DAVARA RODRÍGUEZ, Miguel. Davara & Davara, Asesores Jurídicos. www.davara.com. Visita 20 de Septiembre 2007

[18] GÓMEZ FLOREZ, Luís C. Auditoría de sistemas de información. Grupo de investigación STI, UIS. Bucaramanga, Colombia. 2004.

[19] PALAZZI, Pablo A. Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado. EN: Derecho de Internet & Telecomunicaciones. Colombia. Legis. 2003

[20] Revista de Derecho Informático – Selección de Artículos de Privacidad. http://www.alfa-redi.com/area_tematica.shtml?x=133

ANEXO A

Contenido del documento de políticas de seguridad de los datos

Este documento ha sido diseñado por los desarrolladores del proyecto de investigación, como una guía para la realización del documento de políticas de seguridad de los datos para la dependencia de ARCA o cualquier otra organización.

1 Objetivo del documento de seguridad

En este documento se deben exponer las medidas, políticas, reglas y procedimientos de seguridad adoptadas por la organización, en este caso para la dependencia de ARCA para el procesamiento de los datos de carácter personal, los sistemas de información y para las personas que acceden a estos y a los datos; este documento debe ser de carácter privado y de obligado cumplimiento para todo el personal que accede a los sistemas de información que operan datos personales. Además de lo anterior se debe hacer referencia al nombre del sistema de información o las bases de datos que manejan estos datos.

2 Ámbito de aplicación

En este apartado se describe que el documento será de aplicación para los sistemas de información que contengan datos de carácter personal, soportes informáticos, equipos para el procesamiento y almacenamiento de los datos, personal que tiene acceso a los datos y los locales en donde se operan o ubican los equipos de cómputo.

3 Recursos protegidos

Describir claramente los siguientes aspectos:

3.1 Sistemas de información, programas y aplicaciones informáticas utilizadas para el tratamiento de datos de carácter personal.

3.2 Equipos informáticos que almacenan datos personales (servidores, terminales)

3.3 Lugar o ubicación donde se encuentran los centros y demás equipos de cómputo (ordenadores, equipos y servidores que almacenan la información) y el personal que utiliza los datos

3.4 Descripción de la red de comunicaciones

3.5 Personal que acceden a los datos de acuerdo a sus funciones y obligaciones, que intervienen en cualquiera de las etapas del procesamiento de los datos (recolección, procesamiento, almacenamiento y utilización de datos)

4 Medidas, normas, procedimientos reglas y estándares de seguridad

Describir las medidas de seguridad adoptadas por la dependencia, las cuales como mínimas deben ser:

4.1 Procedimientos y normas de acceso a los sistemas de información

En esta sección incluir y detallar los controles de acceso a los sistemas de información, de los cuales se debe registrar la identificación del usuario, fecha y hora en que se realizó, la base de datos accedida, el tipo de acceso y si este ha sido autorizado o denegado. De igual forma se debe especificar por cuanto tiempo se conservarán los datos de los registros de accesos, el cual no debe ser menor a un periodo de dos años. Es obligación del responsable de la seguridad o el administrador del sistema, revisar periódicamente la información de control registrada e informar al director de la dependencia cualquier anomalía o acceso no autorizado.

Se debe tener en cuenta que el personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Por lo tanto se debe realizar una relación de usuarios con acceso autorizados al sistema y su rol de trabajo dentro de la dependencia, e incluir el tipo de acceso autorizado o perfil para cada uno de ellos. Se recomienda que esta lista esté siempre actualizada y detallada como un anexo de este documento de seguridad.

4.2 Procedimientos y normas para la identificación y autenticación del personal autorizado para acceder a los sistemas

Teniendo en cuenta que en la dependencia de ARCA, la autenticación de los usuarios en el sistema se realiza por medio de contraseñas; en este apartado se debe detallar y especificar el procedimiento de asignación, distribución y almacenamiento e indicar la periodicidad con las que se deberán cambiar. De igual forma incluir los requisitos de complejidad que deben cumplir las cadenas utilizadas como contraseñas.

4.3 Procedimientos y medidas de seguridad lógica utilizadas para la defensa ante ataques externos

En esta sección se describen las características del programa antivirus utilizado, firewalls, cifrado de redes, control de puertos, u otros mecanismos utilizados por la dependencia para evitar ataques externos.

4.4 Procedimientos, normas y controles de acceso a través de redes de telecomunicaciones

Las normas de seguridad adoptadas por la dependencia a los accesos de datos de carácter personal a través de redes de telecomunicaciones deberán garantizar un nivel de seguridad equivalente los accesos locales; para estos accesos la dependencia debe tener en cuenta:

- Sistema de autenticación mediante contraseñas, cifrado de la información u otro método que brinde seguridad al acceso
- Protecciones físicas de acceso a las terminales de trabajo, servidores, equipos de comunicaciones y cableado.
- Bloqueos o limitación en el número de intentos fallidos.
- Selección y utilización de buenos equipos de comunicación como routers, switch, hubs, proxies, gateways y de protección como el firewall.

Además, se deben hacer evaluaciones de riesgo periódicas y analizar los posibles puntos débiles; analizar periódicamente los registros de acceso, por lo menos los que presenten alguna anomalía.

4.5 Normas de acceso físico a los centros de computo

Realizar una breve descripción de los mecanismos o controles de acceso físico del personal a locales y oficinas donde están ubicados los equipos de computo (cámaras, vigilantes, entre otros)

4.6 Gestión de soportes

Los soportes informáticos que contienen datos personales, deben ser inventariados y almacenados para permitir su identificación y conocer más rápidamente que tipo de datos contiene; en esta sección del documento se deben indicar las normas para rotular dichos soportes, especificar el procedimiento para inventariar y almacenar los mismos, indicar el lugar de acceso restringido donde se almacenarán y las personas que tienen acceso al lugar y a estos soportes.

De igual forma se debe detallar el procedimiento a seguir para la salida de estos fuera de la dependencia, lo cual solo podrá ser autorizado por el director de esta; se debe registrar la entrada y salida de los soportes, el cual puede ser manual o informático, para la entrada de soportes a la dependencia, en este registro debe constar el tipo de soporte, fecha y hora, responsable y forma de envió, el número de soportes, el tipo de información que contienen, y la persona que recibe, para el caso de las salidas, el tipo de soporte, fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega. Estas medidas también se deben adoptar para las operaciones de mantenimiento de los equipos,

si en algún momento estas se realizan fuera de las oficinas de la dependencia y en caso que estos almacenen datos personales confidenciales.

Se debe tener en cuenta como soportes documentos, cartas, informes, volantes, comprobantes, entre otros y como soportes informáticos los cd's, memorias usb, diskette, computadores portátiles y demás dispositivos móviles que puedan contener datos personales.

4.7 Creación de bases de datos temporales

Los archivos o bases de datos temporales deberán cumplir con todas las políticas de seguridad implantadas por la dependencia y deben ser borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

4.8 Copias de seguridad

Es obligatorio realizar las copias de seguridad o backup de las bases de datos que contienen información personal. Más adelante se detallará este aspecto; sin embargo esta es otra medida que se debe tomar como seguridad para los datos.

4.9 Funciones y obligaciones del personal

Todo el personal que acceda a los datos de carácter personal está obligado a conocer las medidas, procedimientos, y estándares que afecten a las funciones que desarrolla, de igual forma deben guardar confidencialidad sobre los datos personales que accedan o utilizan en el desarrollo de su trabajo.

Hay dos categorías de personal que utilizan o acceden a los datos:

- **Administradores del sistema**, que son responsables de administrar los sistemas o bases de datos.
- **Usuarios del sistema**, es el personal que utiliza el sistema de información para acceder a los datos.

Se debe describir las principales funciones y obligaciones para los administradores y usuarios del sistema, los cuales son los que acceden a los datos contenidos en bases de datos, de igual forma, definir los tipos de acceso al sistema; estos usuarios deben ser clasificados por grupos de usuarios, por perfiles de usuarios o por funciones laborales, se deben incluir las obligaciones, cargo y perfiles de forma detallada para cada una de las personas, se aconseja que estas listas de usuarios se mantengan siempre actualizadas; en éste apartado también se deben definir los procedimientos para delegar funciones en casos de ausencia.

5 Estructura de la base de datos y descripción de los sistemas de información que tratan datos de carácter personal.

Describir los sistemas de información y demás aplicaciones o tecnologías que se utilizan para el procesamiento de datos personales o cualquier otro dato relevante al sistema. Como anexo al documento de seguridad se puede colocar la documentación del sistema; así mismo, se puede tener como anexo un inventario de hardware, software y de las bases de datos, los cuales pueden contener:

- **Inventario hardware**
  Nombre del equipo (Nombre interno), marca, modelo, serie, sistema operativo y ubicación.

- **Inventario software**
  Aplicación, versión, función, módulos, lenguaje, fecha de creación, fecha de modificación

- **Inventario base de datos**
  Base de datos, sistema gestor de base de datos (SGBD), entorno (cliente servidor, distribuidor) y las tablas o entidades que contiene

6 Configuración del sistema informático

En esta sección se puede incluir un gráfico que represente la ubicación de las diferentes conexiones de los elementos del sistema de información, incluyendo los elementos de seguridad como los servidores, firewall, routers y demás elementos utilizados.

Conocer la ubicación de cada uno de los elementos que componen el sistema de información y las conexiones entre ellos mismos, es muy importante para la dependencia, ya que esta información es necesaria al momento de realizar modificaciones en la arquitectura del sistema.

7 Procedimiento de notificación, gestión y respuesta ante incidencias

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda originar un peligro para la seguridad de los sistemas, y la confidencialidad, integridad y disponibilidad de los datos.

El mantener un registro de las incidencias que comprometan la seguridad de un sistema es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para persecución de los responsables de los mismos.

Este apartado debe contener un registro de incidencias en el que se describa:

- Tipo de incidencia
- Momento en que ocurre
- Persona que realiza el informe
- Persona a quien se le comunica
- Efectos derivados de la incidencia

8 Procedimientos de realización de copias de seguridad y recuperación de datos

Establecer y definir cuándo, cómo y qué procedimiento utilizar para realizar las copias de seguridad, de igual forma definir el procedimiento a seguir en la restauración de datos.

ANEXO B

REAL DECRETO 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

El artículo 18.4 de la Constitución Española establece que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, prevé en su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el artículo 43.3.h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen constituye infracción grave en los términos previstos en la propia Ley.

Sin embargo, la falta de desarrollo reglamentario ha impedido disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consecuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica. El presente Reglamento tiene por objeto el desarrollo de lo dispuesto en los artículos 9 y 43.3.h) de la Ley Orgánica 5/1992. El Reglamento determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor.

En su virtud, a propuesta de la Ministra de Justicia, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 11 de junio de 1999,

DISPONGO:

Artículo único. Aprobación del Reglamento.

Se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, cuyo texto se inserta a continuación.

Disposición final única. Entrada en vigor.

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el “Boletín Oficial del Estado”.

Dado en Madrid a 11 de junio de 1999.

JUAN CARLOS R.

La Ministra de Justicia,
MARGARITA MARISCAL DE GANTE Y MIRÓN

REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL

CAPÍTULO I

Disposiciones generales

Artículo 1. Ámbito de aplicación y fines.

El presente Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Artículo 2. Definiciones.

A efectos de este Reglamento, se entenderá por:

1. Sistemas de información: conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

2. Usuario: sujeto o proceso autorizado para acceder a datos o recursos.

3. Recurso: cualquier parte componente de un sistema de información.

4. Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

5. Identificación: procedimiento de reconocimiento de la identidad de un usuario.

6. Autenticación: procedimiento de comprobación de la identidad de un usuario.

7. Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

8. Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

9. Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

10. Soporte: objeto físico susceptible de ser tratado en un sistema informático y sobre el cual se pueden grabar o recuperar datos.

11. Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

12. Copia del respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Artículo 3. Niveles de seguridad.

1. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.

2. Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información

Artículo 4. Aplicación de los niveles de seguridad.

1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.

5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

Artículo 5. Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Artículo 6. Régimen de trabajo fuera de los locales de la ubicación del fichero.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Artículo 7. Ficheros temporales.

1. Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento.

2. Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Medidas de seguridad de nivel básico

Artículo 8. Documento de seguridad.

1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal, y a los sistemas de información.

2. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.

c) Funciones y obligaciones del personal.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

3. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

4. El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Artículo 9. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas de acuerdo con lo previsto en el artículo 8.2.c).

2. El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 10. Registro de incidencias.

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se han derivado de la misma.

Artículo 11. Identificación y autenticación.

1. El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

2. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

3. Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Artículo 12. Control de acceso.

1. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a información o recursos con derechos distintos de los autorizados.

3. La relación de usuarios a la que se refiere el artículo 11.1 de este Reglamento contendrá el acceso autorizado para cada uno de ellos.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos conforme a los criterios establecidos por el responsable del fichero.

Artículo 13. Gestión de soportes.

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

Artículo 14. Copias de respaldo y recuperación.

1. El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en el que se encontraban al tiempo de producirse la pérdida o destrucción.

3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

CAPÍTULO III

Medidas de seguridad de nivel medio

Artículo 15. Documento de seguridad.

El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Artículo 16. Responsable de seguridad.

1. El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.

Artículo 17. Auditoría.

1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Artículo 18. Identificación y autenticación.

1. El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizado de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

2. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 19. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Artículo 20. Gestión de soportes.

1. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita , directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada

3. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán, las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

4. Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Artículo 21. Registro de incidencias.

1. En el registro regulado en el artículo 10 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 22. Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

CAPÍTULO IV

Medidas de seguridad de nivel alto

Artículo 23. Distribución de soportes.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Artículo 24. Registro de accesos.

1. De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Artículo 25. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

Artículo 26. Telecomunicaciones.

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO V

Infracciones y sanciones

Artículo 27. Infracciones y sanciones.

1. El incumplimiento de las medidas de seguridad descritas en el presente Reglamento será sancionado de acuerdo con lo establecido en los artículos 43 y 44 de la Ley Orgánica 5/1992, cuando se trate de ficheros de titularidad privada.
El procedimiento a seguir para la imposición de la sanción a la que se refiere el párrafo anterior será el establecido en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45, de la Ley Orgánica 5/1992.

Artículo 28. Responsables.

Los responsables de los ficheros, sujetos al régimen sancionador de la Ley Orgánica 5/1992, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal en los términos establecidos en el presente Reglamento.

CAPÍTULO VI

Competencias del Director de la Agencia de Protección de Datos

Artículo 29. Competencias del Director de la Agencia de Protección de Datos.

El Director de la Agencia de Protección de Datos podrá, de conformidad con lo establecido en el artículo 36 de la Ley Orgánica 5/1992:

1. Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica 5/1992.

2. Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se cumplan las medidas de seguridad previstas en el presente Reglamento.

Disposición transitoria única*. Plazos de implantación de las medidas*.

En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años.

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Reglamento.